

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENTS

Applicants: Satoko Tonegawa, et al.

Serial No.: unassigned

Art Unit: unassigned

Filed: herewith

Docket: 13458

(JP9 1999-0060)

For: ALTERATION DETECTION APPARATUS
AND METHOD THEREOF

Dated: April 12, 2000


Assistant Commissioner for Patents
Washington, DC 20231

CLAIM OF PRIORITY

Sir:

Applicants, in the above-identified application, hereby claim the right of priority in connection with Title 35 U.S.C. §119 and in support thereof, herewith submits certified copies of Japanese Patent Application No. 11-107055, filed on April 14, 1999 and Japanese Patent Application No. 11-158358, filed on June 4, 1999.

Respectfully submitted,


Richard L. Catania
Registration No. 32,608

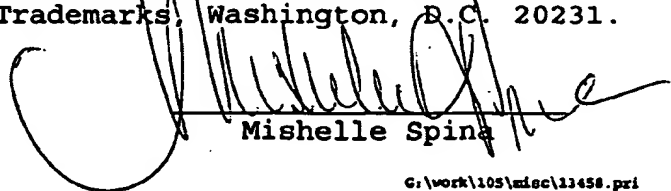
Scully, Scott, Murphy & Presser
400 Garden City Plaza
Garden City, NY 11530
(516) 742-4343
RLC:vjs

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" Mailing Label Number: EL357933192US
Date of Deposit: April 12, 2000

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Dated: April 12, 2000


Mishelle Spina

G:\work\105\misc\13458.pri

10398 U.S. PRO
09/548377
04/12/00

JA 999 060

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

1-398 U.S. PTO
09/548377
04/12/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 4月14日

願 番 号
Application Number:

平成11年特許願第107055号

願 人
Applicant(s):

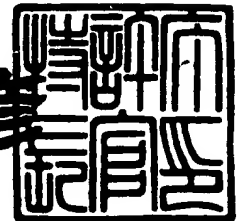
インターナショナル・ビジネス・マシーンス・コーポレイシ
ョン

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年11月26日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



【書類名】 特許願

【整理番号】 JA999060

【あて先】 特許庁長官 殿

【国際特許分類】 H04N 7/167
H04N 5/225

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1623 番地 14 日本アイ・ピー・エム株式会社 大和事業所内

【氏名】 利根川 聡子

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1623 番地 14 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 森本 典繁

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1623 番地 14 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 上條 浩一

【特許出願人】

【識別番号】 390009531

【住所又は居所】 アメリカ合衆国 10504、ニューヨーク州アーモンク
(番地なし)

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【連絡先】 0462-73-3318、3325、3455

【選任した代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【手数料の表示】

【予納台帳番号】 024154

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304391

【包括委任状番号】 9304392

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 改変判定装置およびその方法

【特許請求の範囲】

【請求項 1】

所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定する判定装置とを有するコンテンツ改変判定装置であって、

前記データ付加装置は、

前記コンテンツデータを複数の第 1 のブロックに分割するコンテンツデータ分割手段と、

分割の結果として得られた前記複数の第 1 のブロックそれぞれに、所定の第 1 の埋め込みデータそれぞれを付加し、複数の第 2 のブロックとする埋め込みデータ付加手段と

を有し

前記判定装置は、

前記第 2 のブロックそれぞれに付加された前記埋め込みデータ（第 2 の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、

抽出された前記第 2 の埋め込みデータに基づいて、前記第 2 のブロックそれぞれに改変が加えられたか否かを判定する改変判定手段と

を有する

改変判定装置。

【請求項 2】

画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、

前記データ付加装置は、

画像データを複数の第 1 の画像ブロックに分割する画像分割手段と、

分割の結果として得られた前記複数の第 1 の画像ブロックそれぞれに、所定の

第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加手段と

を有し、

前記判定装置は、

前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、

抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段と

を有する

改変判定装置。

【請求項3】

前記画像分割手段は、前記画像データを、それぞれ複数の単位データを含む前記複数の第1の画像ブロックに分割し、

前記埋め込みデータ付加手段は、互いに対応する2つ以上の前記第1の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第1の埋め込みデータを表すように調整して、前記複数の第1の画像ブロックそれぞれに前記第1の埋め込みデータを付加することにより、前記第2の画像ブロックとする

請求項2に記載の改変判定装置。

【請求項4】

前記埋め込みデータ付加手段は、いずれかの前記第2の画像ブロックに対して改変が加えられた場合に、改変が加えられた前記第2の画像ブロックに含まれ、互いに対応する前記複数の単位データの値が、前記所定の規則に従わなくなるように調整する

請求項3に記載の改変判定装置。

【請求項5】

前記埋め込みデータ抽出手段は、前記複数の第2の画像ブロックそれぞれから、前記第2の画像ブロックそれぞれに含まれる前記複数の単位データの値の関係が、前記所定の規則に従って表すデータを、前記第2の埋め込みデータとして抽

出する

請求項 4 に記載の改変判定装置。

【請求項 6】

前記改変判定手段は、埋め込まれた前記第 1 の埋め込みデータと、抽出された前記第 2 の埋め込みデータとの比較結果に基づいて、前記第 2 の画像ブロックそれぞれに改変が加えられたか否かを判定する

請求項 5 に記載の改変判定装置。

【請求項 7】

前記第 1 の画像ブロックおよび前記第 2 の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の処理ブロックに分割し、空間領域から周波数領域に変換処理することにより得られる複数の変換係数を 1 組以上、含む変換ブロックである

請求項 2～6 のいずれかに記載の改変判定装置。

【請求項 8】

前記第 1 の画像ブロックおよび前記第 2 の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の DCT ブロックに分割し、離散的余弦変換（DCT）処理することにより得られる複数の DCT 係数を 1 組以上、含む DCT ブロックである

請求項 2～7 のいずれかに記載の改変判定装置。

【請求項 9】

画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置であって、前記判定は、前記画像データに含まれる複数の第 2 の画像ブロックそれぞれに付加された第 2 の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、

前記データ付加装置は、

画像データを複数の第 1 の画像ブロックに分割する画像分割手段と、

分割の結果として得られた前記複数の第 1 の画像ブロックそれぞれに、所定の第 1 の埋め込みデータそれぞれを付加し、前記複数の第 2 の画像ブロックとする

埋め込みデータ付加手段と

を有するデータ付加装置。

【請求項 10】

前記画像分割手段は、前記画像データを、それぞれ複数の単位データを含む前記複数の第1の画像ブロックに分割し、

前記埋め込みデータ付加手段は、互いに対応する2つ以上の前記第1の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第1の埋め込みデータを表すように調整して、前記複数の第1の画像ブロックそれぞれに前記第1の埋め込みデータを付加することにより、前記第2の画像ブロックとする

請求項9に記載のデータ付加装置。

【請求項 11】

前記埋め込みデータ付加手段は、いずれかの前記第2の画像ブロックに対して改変が加えられた場合に、改変が加えられた前記第2の画像ブロックそれぞれに含まれ、互いに対応する前記複数の単位データの値が、前記所定の規則に従わなくなるように調整する

請求項10に記載のデータ付加装置。

【請求項 12】

画像データを複数の第1の画像ブロックに分割し、分割の結果として得られた前記第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加することにより作られた複数の第2の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置であって、

前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、

抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段と

を有する判定装置。

【請求項 13】

前記画像データは、それぞれ複数の単位データを含む前記複数の第1の画像ブ

ロックに分割され、前記第2の画像ブロックは、互いに対応する2つ以上の前記第1の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第1の埋め込みデータを表すように調整され、

前記埋め込みデータ抽出手段は、前記複数の第2の画像ブロックから、対応する前記2つ以上の第2の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、前記所定の規則に従って表すデータを、前記第2の埋め込みデータとして抽出する

請求項12に記載の判定装置。

【請求項14】

いずれかの前記第2の画像ブロックに対して改変が加えられた場合には、改変が加えられた前記第2の画像ブロックそれぞれに含まれ、互いに対応する前記複数の単位データの値は、前記所定の規則に従わなくなるように調整され、

前記改変判定手段は、埋め込まれた前記第1の埋め込みデータと、抽出された前記第2の埋め込みデータとの比較結果に基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する

請求項13に記載の判定装置。

【請求項15】

改変が加えられたと判定された前記第2の画像ブロックの位置が、この画像内において占める位置を表示する改変位置表示手段

をさらに有する請求項12～14のいずれかに記載の判定装置。

【請求項16】

所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加し、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定するコンテンツ改変判定方法であって、

前記コンテンツデータを複数の第1のブロックに分割し、

分割の結果として得られた前記複数の第1のブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2のブロックとし、

前記第2のブロックそれぞれに付加された前記埋め込みデータ（第2の埋め込

みデータ)を抽出し、

抽出された前記第2の埋め込みデータに基づいて、前記第2のブロックそれぞれに改変が加えられたか否かを判定する

改変判定方法。

【請求項17】

画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置において、

画像データを複数の第1の画像ブロックに分割する画像分割ステップと、

分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加ステップと、

前記第2の画像ブロックそれぞれに付加された埋め込みデータ(第2の埋め込みデータ)を抽出する埋め込みデータ抽出ステップと、

抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップと

をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項18】

画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置において、前記判定は、前記画像データに含まれる複数の第2の画像ブロックそれぞれに付加された第2の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、

画像データを複数の第1の画像ブロックに分割する画像分割ステップと、

分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、前記複数の第2の画像ブロックとする埋め込みデータ付加ステップと

をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項19】

画像データを複数の第1の画像ブロックに分割し、分割の結果として得られた前記第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加することにより作られた複数の第2の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置において、

前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出ステップと、

抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップと

をコンピュータに実行させるプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】

本発明は、著作権情報などの認証情報を、画像データ等のコンテンツデータに感知できないように認証データを埋め込み、埋め込んだ認証データを用いてコンテンツのいずれの部分に改変が加えられたかを判定する改変判定装置およびその方法に関する。

【0002】

【従来の技術】

例えば、国際公開WO97/49235号公報（文献1）は、ピクセル・ブロック・コーディング（Pixel Block Coding；PBC）により、画像データ等のコンテンツデータに著作権情報など（以下、一般的に認証情報とも記す）を、視覚的に感知できないように埋め込む方式（以下、このようにコンテンツデータに感知できないように認証方法を埋め込む方式を「エレクトロニックウォーターマーキング方式」とも記す）を開示する。

【0003】

また、国際公開WO98/116928号公報（文献2）は、文献1等を開示されたエレクトロニックウォーターマーキング方式を応用して、画像データの改変を禁止し、著作物を有効に保護する方法を開示する。

また、特開平10-164549号公報（文献3）は、文献1等を開示された

エレクトロニックウォーターマーキング方式を改良し、画像データに認証情報を一体不可分に埋め込むことにより、画像データの改変を検出する方法を開示する。

【0004】

また、これらの文献の他、特開平09-151747号公報、特開平10-83310号公報、特開平10-106149号公報、特開平10-161933号公報、特開平10-164349号公報、特開平10-285562号公報、特開平10-334272号公報、特開平10-240626号公報、特開平10-240129号公報（文献4～12）等も、エレクトロニックウォーターマーキング方式に関する発明を開示する。

【0005】

これらの文献に開示された方式は、ハッシュ関数等を用いて認証情報を埋め込み、画像データに改変が加えられているか否かを判断する。ハッシュ関数を用いて認証情報を埋め込まれた画像データの一部に対して改変を行うと、この改変の影響は画像データ全体に及ぶ。従って、この方式は、画像データのいずこかに改変が加えられていることを検出することができても、具体的に、画像データのいずれの部分に改変が加えられているかを判定して示すことはできない。

【0006】

【発明が解決しようとする課題】

本発明は、上述した従来技術の問題点に鑑みてなされたものであり、単にコンテンツデータに対して改変が加えられているか否かを判定することができるだけでなく、さらに、コンテンツデータのいずれの部分に改変が加えられているかまでを判定することができるようにした改変判定装置およびその方法を提供することを目的とする。

【0007】

【課題を達成するための手段】

〔改変判定装置〕

本発明にかかるコンテンツ改変判定装置は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加するデータ付加装置と

、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定する判定装置とを有するコンテンツ改変判定装置であって、前記データ付加装置は、前記コンテンツデータを複数の第1のブロックに分割するコンテンツデータ分割手段と、分割の結果として得られた前記複数の第1のブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2のブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第2のブロックそれぞれに付加された前記埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、抽出された前記第2の埋め込みデータに基づいて、前記第2のブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【0008】

好適には、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、前記データ付加装置は、画像データを複数の第1の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【0009】

好適には、前記画像分割手段は、前記画像データを、それぞれ複数の単位データを含む前記複数の第1の画像ブロックに分割し、前記埋め込みデータ付加手段は、互いに対応する2つ以上の前記第1の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第1の埋め込みデータを表すように調整して、前記複数の第1の画像ブロックそれぞれに前記第1の埋め込みデータを付加することにより、前記第2の画像ブロックとする。

【 0 0 1 0 】

好適には、前記埋め込みデータ付加手段は、いずれかの前記第 2 の画像ブロックに対して改変が加えられた場合に、改変が加えられた前記第 2 の画像ブロックに含まれ、互いに対応する前記複数の単位データの値が、前記所定の規則に従わなくなるように調整する。

【 0 0 1 1 】

好適には、前記埋め込みデータ抽出手段は、前記複数の第 2 の画像ブロックそれぞれから、前記第 2 の画像ブロックそれぞれに含まれる前記複数の単位データの値の関係が、前記所定の規則に従って表すデータを、前記第 2 の埋め込みデータとして抽出する。

【 0 0 1 2 】

好適には、前記改変判定手段は、埋め込まれた前記第 1 の埋め込みデータと、抽出された前記第 2 の埋め込みデータとの比較結果に基づいて、前記第 2 の画像ブロックそれぞれに改変が加えられたか否かを判定する。

【 0 0 1 3 】

好適には、前記第 1 の画像ブロックおよび前記第 2 の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の処理ブロックに分割し、空間領域から周波数領域に変換処理することにより得られる複数の変換係数を 1 組以上、含む変換ブロックである。

【 0 0 1 4 】

好適には、前記第 1 の画像ブロックおよび前記第 2 の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の D C T ブロックに分割し、離散的余弦変換 (D C T) 処理することにより得られる複数の D C T 係数を 1 組以上、含む D C T ブロックである。

【 0 0 1 5 】

〔改変判定装置の作用〕

本発明にかかる判定装置は、例えば、事故調査に用いられる事故現場の音声データあるいは画像データといった、改変が加えられると証拠として用いることができないコンテンツデータに、予め、改変の判定に用いる埋め込みデータ（いわ

ゆる電子透かし（エレクトロニックウォーターマーク）を埋め込んでおき、埋め込んだ埋め込みデータを用いて、コンテンツデータのいずれの部分に改変が加えられたかを判定する。

【0016】

より具体的には、本発明にかかる判定装置は、例えば、それぞれDCT係数を2組ずつ含む複数のペア（画像ブロック）に分割し、これらのペアそれぞれに対して、電子透かしを、ペアごとに改変の判定が可能なように埋め込んでおき、画像データが改変されたか否かを判定する際に、この判定を、ペアごとに行うことにより、画像データに改変が加えられたか否か、および、画像データのいずれの部分に改変が加えられたかを判定する。

【0017】

本発明にかかる判定装置による埋め込みデータ（電子透かし）の埋め込みの対象となるDCT係数としては、例えば、カラー画像データの輝度成分（Y）を、8×8画素構成の複数のDCTブロック（マクロブロック）にし、これらのDCTブロックをDCT処理して得られるDCT係数が用いられる。

【0018】

DCT係数のペアはそれぞれ、例えば、乱数を用いてランダムに選択された複数組のDCT係数、あるいは、単純に隣り合った複数組のDCT係数を含む。

なお、以下、説明の明確化・簡略化のため、特に断らない限り、これらの例の内、後者の例の最も単純な場合、つまり、DCT係数のペアそれぞれが、単純に隣り合った2つのDCTブロックをDCT変換して得られる2組の（隣接した2つの）DCT係数を含む場合を具体例として説明を進める。

【0019】

〔データ付加装置〕

本発明にかかる改変判定装置において、データ付加手段は、画像データに対して、DCT係数のペアごとに改変の判定が可能なように、埋め込みデータ（電子透かし）の埋め込みを行う。

【0020】

〔画像分割手段〕

データ付加手段において、画像分割手段は、例えば、J P E G方式により圧縮符号化された圧縮画像データをハフマン復号処理し、復号処理の結果として得られた画像データの3種類の成分の内、輝度成分（Y）のD C T係数を受け入れ、隣り合った2組のD C T係数同士に対応付け、対応付けた2組のD C T係数から構成されるペア（第1の画像ブロック）とする。

【0021】

[埋め込みデータ付加手段]

埋め込みデータ付加手段は、ペア（第1の画像ブロック）それぞれに含まれる2組のD C T係数の内の1つ以上（単位データ）を、相互に対応付けて取り出す（なお、2組のD C T係数それぞれから1つ以上取り出されるので、1つのペアからは複数の単位データが選択される）。

また、埋め込みデータ付加手段は、例えば、鍵情報を用いて乱数を発生し、発生した乱数を用いて、例えば、96ビットの埋め込みデータをスクランブル処理する。

また、埋め込みデータ付加手段は、ペア（第1の画像ブロック）それぞれと、スクランブルされた埋め込みデータ（第1の埋め込みデータ）の各ビットとを対応付ける。

【0022】

さらに、埋め込みデータ付加手段は、ペア（第1の画像ブロック）に含まれる2組のD C T係数それぞれから取り出され、これら2組のD C T係数の間で相互に対応するD C T係数（単位データ）同士の関係が、所定の規則に従って、これらのD C T係数が含まれていたペア（第1の画像ブロック）に対応付けられた埋め込みデータのビット（第1の埋め込みデータ）の値（1または0）を表すように、これらのD C T係数の値を調整することにより、埋め込みデータを埋め込む。

【0023】

なお、ペア（第1の画像ブロック）に含まれる2組のD C T係数から、D C T係数を選択する方法は、例えば、予め設定された固定の対応関係に基づいてD C T係数を選択する方法であっても、乱数に基づいてランダムにD C T係数に対応

付けて選択する係数であってもよい。

なお、以下、説明の明確化のために、特に断らない限り、各ペア（第1の画像ブロック）に含まれる2組のDCT係数それぞれから、ペアごとに乱数を用いてランダムに、互いに対応する3個ずつ（合計6個）のDCT係数を選択する場合、つまり、ペアが異なれば、異なった位置からDCT係数が選択されるが、同じペアに含まれるDCT係数からは、同じ位置のDCT係数が選択される場合を具体例にして説明を行う。

【0024】

このように各ペアに、埋め込みデータのビットを埋め込むと、例えば、ハッシュ関数を用いて埋め込みデータを埋め込んだ場合と異なり、あるペアに対して加えられた改変は、そのペア以外に影響を与えない。

つまり、このように埋め込みをおこなうと、画像の一部に対する改変の影響は、画像の他の部分に及ばないので、画像に加えられた改変を、部分ごとに判定することができる。

【0025】

〔判定装置〕

埋め込みデータ（第1の埋め込みデータ）の各ビットが埋め込まれた後に、例えば、画像データの一部を塗りつぶし、写っていた物体が消去されるといった改変が加えられると、改変が加えられた部分のペア（第2の画像ブロック）に含まれ、相互に対応するDCT係数（単位データ）同士の関係が、上記所定の規則から外れることとなり、その埋め込みデータのビット（第2の埋め込みデータ）は、埋め込まれたときの埋込データのビット（第1の埋め込みデータ）と異なる値を示すことになる。

【0026】

また、例えば、96ビットの埋め込みデータ（第1の埋め込みデータ）を、1024ビット×768ビット構成の画像を構成する6144組のDCT係数のペア（第1の画像ブロック）に埋め込むと、埋め込みデータ（第1の埋め込みデータ）の各ビットが64回ずつ、1つの画像データに埋め込まれることになる。

【0027】

一方、画像データの比較的、小面積の部分に対してのみ、改変が加えられた場合、改変が加えられた部分において、対応する埋め込みデータ（第1の埋め込みデータ）のビットを表さなくなるペアの数は、改変が加えられなかった部分において、対応する埋め込みデータ（第1の埋め込みデータ）のビットを表わしているペアの数よりも少なくなるはずである。

【0028】

従って、改変が加えられた可能性がある画像から埋め込みデータ（第2の埋め込みデータ）を抽出し、抽出した埋め込みデータ（第2の埋め込みデータ）の内、埋め込みデータ（第1の埋め込みデータ）の同じビットに対応する64個のペア（第2の画像ブロック）それぞれが、上記所定の規則に従って、1, 0いずれの値を表しているかの多数決を採ると、多数のペアが表している値を、データ付加装置が付加した埋め込みデータ（第1の埋め込みデータ）の値であると判断することができる。

同様に、この多数決の結果、少数となったペア（第2の画像ブロック）の位置に、改変が加えられたと推定することができる。

【0029】

本発明にかかる判定装置は、このような埋め込みデータの性質を利用し、改変が加えられた可能性があるDCT係数のペア（第2の埋め込みデータ）それぞれから、改変が加えられた結果、埋め込まれた当初とは値が変更されている可能性がある埋め込みデータ（第2の埋め込みデータ）を抽出する。

さらに、判定装置は、この抽出結果に基づいて、DCT係数のペア（第2の画像ブロック）のいずれに改変が加えられているか、つまり、画像データのいずれの部分に改変が加えられているかを判定する。

【0030】

[埋め込みデータ抽出手段]

埋め込みデータ抽出手段は、本発明にかかるデータ付加装置により埋め込みデータ（第1の埋め込みデータ）が埋め込まれた後に改変が加えられた可能性があるペア（第2の画像ブロック）の2組のDCT係数それぞれに含まれ、相互に対応するDCT係数（単位データ）が、上記所定の規則に従って表す値（第2の埋

め込みデータ)を抽出する。

【0031】

〔改変判定手段〕

改変判定手段は、埋め込みデータの同じビットに対応する複数のペア（第2の画像ブロック）が、1，0いずれの値を表すかの多数決を採り、多数のペアが表す値を、埋め込み時の埋め込みデータ（第1の埋め込みデータ）と判定し、この埋め込みデータと異なる値を表すペア（第2の画像ブロック）に対して、改変がなされたと判定する。

【0032】

〔データ付加装置〕

本発明にかかるデータ付加装置は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置であって、前記判定は、前記画像データに含まれる複数の第2の画像ブロックそれぞれに付加された第2の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、前記データ付加装置は、画像データを複数の第1の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、前記複数の第2の画像ブロックとする埋め込みデータ付加手段とを有する。

【0033】

〔判定装置〕

また、本発明にかかる判定装置は、画像データを複数の第1の画像ブロックに分割し、分割の結果として得られた前記第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加することにより作られた複数の第2の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置であって、

前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【0034】

〔改変判定方法〕

本発明にかかる改変判定方法は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加し、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定するコンテンツ改変判定方法であって、前記コンテンツデータを複数の第1のブロックに分割し、分割の結果として得られた前記複数の第1のブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2のブロックとし、前記第2のブロックそれぞれに付加された前記埋め込みデータ（第2の埋め込みデータ）を抽出し、抽出された前記第2の埋め込みデータに基づいて、前記第2のブロックそれぞれに改変が加えられたか否かを判定する。

【0035】

〔記録媒体〕

また、本発明にかかる第1の記録媒体は、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置において、画像データを複数の第1の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第1の画像ブロックそれぞれに、所定の第1の埋め込みデータそれぞれを付加し、複数の第2の画像ブロックとする埋め込みデータ付加ステップと、前記第2の画像ブロックそれぞれに付加された埋め込みデータ（第2の埋め込みデータ）を抽出する埋め込みデータ抽出ステップと、抽出された前記第2の埋め込みデータに基づいて、前記第2の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【0036】

また、本発明にかかる第2の記録媒体は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置において、前記判定は、前記画像データに含まれる複数の第2の画像ブロックそれぞれに付加された第2の埋め込みデータに基づいて、前記画像プロ

ックそれぞれに改変が加えられたか否かを判断することにより行われ、画像データを複数の第 1 の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第 1 の画像ブロックそれぞれに、所定の第 1 の埋め込みデータそれぞれを付加し、前記複数の第 2 の画像ブロックとする埋め込みデータ付加ステップとをコンピュータに実行させるプログラムを記録する。

【0 0 3 7】

また、本発明にかかる第 3 の記録媒体は、画像データを複数の第 1 の画像ブロックに分割し、分割の結果として得られた前記第 1 の画像ブロックそれぞれに、所定の第 1 の埋め込みデータそれぞれを付加することにより作られた複数の第 2 の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置において、前記第 2 の画像ブロックそれぞれに付加された埋め込みデータ（第 2 の埋め込みデータ）を抽出する埋め込みデータ抽出ステップと、抽出された前記第 2 の埋め込みデータに基づいて、前記第 2 の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【0 0 3 8】

【発明の実施の形態】

以下、本発明の実施形態を説明する。

【0 0 3 9】

〔改変判定装置 1〕

図 1 は、本発明にかかる改変判定方法を実現する画像改変判定装置 1 の構成を示す図である。

図 1 に示すように、画像改変判定装置 1 は、CRT 表示装置あるいは液晶表示装置等の表示装置 1 0 0、キーボードおよびマウス等を含む入力装置 1 0 2、デジタルカメラインターフェース I F（カメラ I F）1 0 4、メモリカードインターフェース（メモリカード I F）1 0 6、MO 装置および CD 装置等の記憶装置 1 0 8、および、メモリ 1 1 2 およびマイクロプロセッサ（CPU）1 1 4 等を含むコンピュータ本体（PC 本体）1 1 0 から構成され、必要に応じて、さらに通信装置 1 1 6 が付加される。

【0040】

つまり、画像改変判定装置 1 は、一般的なコンピュータに、カメラ I F 1 0 4 およびメモリカード I F 1 0 6 を付加した構成を採る。

画像改変判定装置 1 は、これらの構成部分により、光磁気ディスク (MO) あるいはコンパクトディスク (CD) 等の記録媒体 1 2 0 に記録されて記憶装置 1 0 8 に供給される埋込・判定プログラム 2 (図 2 を参照して後述する) を、メモリ 1 1 2 にロードして実行し、画像データに対する電子透かし (埋め込みデータ) の埋め込み処理および改変 (人為的に加えられた改変か、データが壊れる等の事故に起因する改変かを問わない) の判定処理を実行する。

【0041】

つまり、画像改変判定装置 1 は、デジタルカメラ 1 4 0 が撮影した画像を、例えば J P E G 方式により圧縮符号化して生成した圧縮画像データを、カメラ I F 1 0 4 を介して受け入れ、あるいは、デジタルカメラ 1 4 0 がメモリカード 1 4 2 に記録した圧縮画像データを、メモリカード I F 1 0 6 を介して受け入れ、受け入れた圧縮画像データに電子透かし (埋め込みデータ) を埋め込み、埋め込んだ電子透かし (埋込データ) を用いて、圧縮画像データのいずれの部分に改変が加えられたかを判定する。

【0042】

[埋込・判定プログラム 2]

図 2 は、図 1 に示した画像改変判定装置 1 が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラム 2 の構成を示す図である。

図 2 に示すように、埋込・判定プログラム 2 は、埋込・抽出部 3、鍵情報データベース (DB) 2 2 および画像データベース (DB) 2 4 から構成され、埋込・抽出部 3 は、埋込データ生成部 2 0、制御部 2 6、埋込部 3 0、抽出部 4 0 および O S 5 0 から構成される。

【0043】

[O S 5 0]

O S 5 0 は、例えば、ウィンドウズ (マイクロソフト社商品名) 等のオペレーティングシステムソフトウェアであって、埋込・判定プログラム 2 の各構成部分

の実行制御を行う。

また、OS 50は、埋込データ生成部 20に対して、メモリカード 142のシリアル番号および時刻等、電子透かし（埋込データ）の生成に必要なデータを供給するなど、埋込・判定プログラム 2の各構成部分の処理に必要とされるデータを供給する。

【0044】

〔制御部 26〕

制御部 26は、表示装置 100に操作用のGUI画像を表示し、表示されたGUI画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・判定プログラム 2の各構成部分に供給する。

また、制御部 26は、受け入れたユーザの操作に応じて、埋込・判定プログラム 2の各構成部分の動作を制御する。

【0045】

〔画像DB 24〕

画像DB 24は、埋込部 30が埋め込みデータを埋め込んだ圧縮画像データ（JPEGデータ）を記憶装置 108に挿入された記録媒体 120、あるいは、メモリカード IF 106に挿入されたメモリカード 142に記憶・管理し、記憶・管理した画像データを読み出して抽出部 40に対して出力する。

【0046】

〔鍵情報DB 22〕

鍵情報DB 22は、画像DB 22が管理するJPEGデータと、埋込部 30が、このJPEGデータへ埋め込みデータを埋め込む際に、乱数を発生させるために用いる鍵（例えば64ビットの数値）とを対応付けて記憶装置 108等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部 30および抽出部 40に対して出力する。

【0047】

〔埋込データ生成部 20〕

埋込データ生成部 20は、OS 50から入力されるメモリのシリアル番号等のデータから、例えば96ビットの埋め込みデータを生成し、埋込部 30に対して

出力する。

【0048】

〔埋込部30〕

図3は、図2に示した埋込部30の構成を示す図である。

図4は、図3に示したデータ埋込部32の構成を示す図である。

図3および図4に示すように、埋込部30は、復号部300、データ埋込部32および符号化部304から構成され、データ埋込部32は、画像分割部320、乱数発生部322、位置決め部324、スクランブル部326および係数操作部328から構成される。

【0049】

〔埋込部30の概要〕

埋込部30は、これらの構成部分により、まず、カラーの圧縮画像データを構成するクロマ成分Cb、Crおよび輝度成分Yの1組8画素×8画素構成（1組64画素）のDCT係数の内、例えば輝度成分YのDCT係数を、それぞれDCT係数2組ずつ含む複数のペア（第1の画像ブロック）とする。

【0050】

埋込部30は、さらに、これらのペアそれぞれに、埋込データ生成部20が発生した96ビットの埋込データを、鍵情報DB22（図2）から供給された鍵情報を用いて、例えば16ビットの線形合同法により発生した乱数に基づいてスクランブルしたデータ（第1の埋め込みデータ；以下、記述の簡略化のために、このように「スクランブルされた埋め込みデータ」を、単に「埋め込みデータ」とも記す）の各ビットを埋め込む。

【0051】

〔埋込部30の詳細〕

図5～図12をさらに参照して、埋込部30の処理の詳細を説明する。

図5は、デジタルカメラ140（図1）が撮影した非圧縮画像データを例示する図である。

図6（A）は、図5に例示した非圧縮画像データの一部を示す図であり、（B）は、（A）に例示した非圧縮画像データ（部分）に含まれるDCTブロック（

マクロブロック)を示す図であり、(C)は、(B)に示したDCTブロックそれぞれに含まれる 8×8 構成の画素を示す図である。

【0052】

なお、本来、DCTブロックと、 8×8 構成のDCT係数とは区別する必要があるが、記述の簡略化のために、以下、特に断らない限り、 8×8 構成のDCT係数をDCTブロックとも記し、 8×8 構成のDCTブロックに含まれる各DCT係数を、DCT係数と記す。

【0053】

デジタルカメラ140(図1)は、例えば、人物および風景を撮影し、図5に例示した非圧縮カラー画像データを生成し、さらに、JPEG方式により圧縮符号化する。

つまり、デジタルカメラ140は、図6(A)～(C)に例示するように、得られた非圧縮画像データに含まれる輝度成分Yおよびクロマ成分Cr, Cbそれぞれを、それぞれ 8×8 (64)個の画素を含むDCTブロック(マクロブロックともいう)に分割し、分割の結果として得られたDCTブロックをDCT変換し、さらに、ハフマン符号化して、JPEG方式の圧縮画像データを生成し、カメラIF104を介して、あるいは、メモ리카ード142およびメモ리카ードIF106を介して、PC本体110(図1)により実行される埋込・判定プログラム2の埋込部30(図2, 3)に対して出力する。

【0054】

図7(A)は、デジタルカメラ140から入力される非圧縮画像データを復号部300がハフマン復号して得られる輝度信号YのDCT係数を示す図であり、(B)は、(A)に示した輝度信号YのDCT係数の内、それぞれ隣り合う2組を対応付ける方法を示す図であり、(C)は、(B)に示した方法により対応付けられたDCT係数のペアを示す図である。

【0055】

埋込部30は、まず、入力されたJPEG方式の圧縮画像データをハフマン復号して輝度成分Yおよびクロマ成分Cr, CbのDCTブロックを得て、得られたこれらのDCTブロックの内、図7(A)に示す輝度成分Yの12288個の

DCTブロック (1, 1~96, 128) を、図 7 (B), (C) に示すように、隣り合う 2 つ (ブロック 1, 2) 同士で 6144 ($12288/2$) 個のペアにする。

埋込部 30 は、このようにして得られた 6144 (96×64) 個のペアそれぞれに、上述のように乱数によりスクランブルされた 96 ビットの埋め込みデータの各ビットを、64 回ずつ繰り返し対応付ける。

【0056】

図 8 は、図 2, 3 に示した埋込部 30 が 1 つのペア (図 7 (A), (B)) に含まれる DCT ブロック (ブロック 1, 2) それぞれから選択した相互に対応する DCT 係数を例示する図である。

なお、図 8 は、ペア i ($1 \leq i \leq 6144$) に含まれる 2 つの DCT ブロック (ブロック 1, 2) それぞれから、同じ位置の 3 個の DCT 係数 (2, 3), (3, 2), (3, 3) が選択された場合を例示する。

【0057】

埋込部 30 は、例えば、鍵情報 DB 22 (図 2) から供給された鍵から上述のように発生した乱数を用いて、図 8 に示すように、DCT ブロック (ブロック 1, 2) 内の相互に対応する 3 つの DCT 係数 ($A_1, A_2, B_1, B_2, C_1, C_2$; 単位データ) を、ペアごとにランダムに選択する。言い換えると、埋込部 30 は、同一のペアに含まれる DCT ブロック (ブロック 1, 2) からは、同じ位置の DCT 係数をビットの埋め込みのために選択するが、異なるペアの間では、異なる位置の DCT 係数を選択する。

【0058】

図 9 (A), (B) は、図 8 に例示したように選択されたブロック 1, 2 それぞれの DCT 係数を、埋め込みデータのビット (値 1) を埋め込むために、DCT 係数の数値を変更する必要がある場合について例示する図である。

図 10 は、図 8 に例示したように選択されたブロック 1, 2 それぞれの DCT 係数を、埋め込みデータのビット (値 1) を埋め込むために、DCT 係数の数値を変更する必要がある場合について例示する図である。

【0059】

埋込部 30 は、例えば、図 8 に例示したように、ペア i の 2 つの DCT ブロック（ブロック 1, 2）から選択した相互に対応する DCT 係数（ $A_1, A_2, B_1, B_2, C_1, C_2$ ）値同士の関係が、図 9（A）,（B）および図 10 に例示するように、上述のようにペアそれぞれに対応付けられた埋め込みデータのビットの値に応じて、下表 1 に例示する規則（規則 1-1, 1-2）に従うように調整することにより、各ペアに、対応する埋め込みデータのビットの値（1, 0）を埋め込む。

【0060】

【表 1】

表 1：DCT 係数の関係を示す規則：

ペアに対応付けられた埋め込みデータのビットの値が 1 である場合：

$$(A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 < C_2) ||$$

$$(A_1 > A_2 \&\& B_1 > B_2 \&\& C_1 < C_2) ||$$

$$(A_1 < A_2 \&\& B_1 > B_2 \&\& C_1 > C_2) ||$$

$$(A_1 > A_2 \&\& B_1 < B_2 \&\& C_1 > C_2)$$

...（規則 1-1）

ペアに対応付けられた埋め込みデータのビットの値が 0 である場合：

$$(A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 > C_2) ||$$

$$(A_1 > A_2 \&\& B_1 < B_2 \&\& C_1 < C_2) ||$$

$$(A_1 < A_2 \&\& B_1 > B_2 \&\& C_1 < C_2) ||$$

$$(A_1 > A_2 \&\& B_1 > B_2 \&\& C_1 > C_2)$$

...（規則 1-2）

ただし、上記規則 1-1, 1-2 において、

$X \&\& Y$ は、条件 X, Y の両方を満たすことを示し、

$X || Y$ は、条件 X, Y のいずれかを満たすことを示す。

【0061】

例えば、図 9（A）に例示するように、ペア i に対応付けられた埋め込みデータのビットの値が 1 あり、ペア i の 2 つの DCT ブロック（ブロック 1, 2）の

相互に対応するDCT係数 ($A_1, A_2, B_1, B_2, C_1, C_2$) の値が、それぞれ 4, 4, 2, 3, 5, 4 である場合、これらのDCT係数の値の関係は、 $A_1 = A_2$ であるため、上記規則 1-1, 1-2 のいずれをも満たさない。

【0062】

そこで、埋込部 30 は、図 9 (B) 内の数字に丸印を付して例示するように、相互に対応するDCT係数 ($A_1, A_2, B_1, B_2, C_1, C_2$) 同士の値の関係が、上記規則 1-1 の ($A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 < C_2$) の条件を満たすことになるように、 A_1 の値を増やして、値 1 の埋め込みデータのビットを埋め込む。

つまり、例えば、値 1 のビットを埋め込む場合に、DCT係数 ($A_1, A_2, B_1, B_2, C_1, C_2$) 同士の値が規則 1-1 を満たさない場合には、常に、これらのDCT係数同士の関係が、上記規則 1-1 の ($A_1 < A_2 \&\& B_1 < B_2 \&\& C_1 < C_2$) の条件を満たすことになるように、DCT係数を調節して、値 1 の埋め込みデータのビットを埋め込む。

【0063】

また、例えば、図 10 に例示するように、ペア i に対応付けられた埋め込みデータのビットの値が 1 あり、ペア i の 2 つのDCTブロック (ブロック 1, 2) の相互に対応するDCT係数 ($A_1, A_2, B_1, B_2, C_1, C_2$) の値が、それぞれ 3, 5, 6, 3, 5, 4 である場合、これらのDCT係数の値の関係は、上記規則 1-1 の条件 ($A_1 < A_2 \&\& B_1 > B_2 \&\& C_1 > C_2$) を満たしている。

従って、この場合には、埋込部 30 は、ペア i の 2 つのDCTブロック (ブロック 1, 2) のDCT係数 ($A_1, A_2, B_1, B_2, C_1, C_2$) の値を変更しない。

【0064】

図 11 は、埋込部 30 (図 2, 3) が、DCTブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。

なお、図 11 には、埋め込みデータビット欄が現れているが、この欄は、埋め込みデータがスクランブル処理されていることを説明するために示したものであり、実際の処理においては用いられない。

ここまで説明した埋込部 30 の埋め込み処理を、さらに図 11 を参照して説明

する。

埋込部 30 は、1024 画素×768 画素構成の画像データ（図 5、6（A）～（C））から得られた 12288 個の DCT ブロックの内、隣り合った 2 つの DCT ブロック同士を対応付けて（図 7（A）～（C））、6144 個のペアを作る。

【0065】

また、埋込部 30 は、埋込データ生成部 20（図 2）から供給される 96 ビットの埋め込みデータを、鍵情報 DB 22 から供給される鍵から作成した乱数でスクランブル処理し、スクランブル処理した 96 ビットの埋め込みデータのビットそれぞれの値（1，0）を、下記方法により 64 回ずつ 6144 個のペアそれぞれに対応付け、図 11 に示すように、埋め込みテーブルの埋め込みデータ割り当て欄に書き込む。

【0066】

[埋め込みデータに対応付け方法]

なお、図 11 に例示するように、連続した 96 ペアごとに、それぞれ異なった順番にスクランブルされた 96 ビットの埋め込みデータの各ビットが対応付けられるので、例えば、第 5 番目のペアと、第 160 番目のペアに、埋め込みデータの第 7 番目のビット（1）が割り当てられる。

以下、同様に、6144 個のペアを、順番に 64 組×96 ペアに分割して得られる各組ごとに異なる順番で、各組に含まれる 96 ペアそれぞれに、96 ビットの埋め込みデータの各ビットが対応付けられる。

【0067】

例えば、96 ビットの埋め込みデータの第 1～第 5 ビットはそれぞれ、第 1～第 96 ペアを含む第 1 組においては、第 11 ペア、第 5 ペア、第 31 ペアおよび第 9 ペアに対応付けられ、第 97～第 192 ペアを含む第 2 組においては、第 99 ペア、第 126、第 100 ペア、第 153 ペアに対応付けられる（後に図 18 に例示）。

【0068】

また、埋込部 30 は、上述のように生成された乱数を用いて、図 8 に例示した

ように、ペアごとに、2つのDCTブロック（ブロック1，2）からいずれのDCT係数（ A_1 ， A_2 ， B_1 ， B_2 ， C_1 ， C_2 ）を取り出すかを決め、取り出したDCT係数の値を、埋め込みテーブルのブロック1，2の欄に書き込む。

上述のように、埋込部30が 8×8 構成のDCT係数のいずれを取り出すかは、ペアごとに一定ではない。

【0069】

以上の処理が終了すると、埋込部30は、各ペアのDCTブロック（ブロック1，2）から選択されたDCT係数（ A_1 ， A_2 ， B_1 ， B_2 ， C_1 ， C_2 ）が、上記表1に示した規則1-1，1-2に基づいて、埋め込みテーブルの埋め込みデータ割り当て欄のビットの値を表すように、埋め込みテーブルのブロック1，2の欄に書き込まれたDCT係数（ A_1 ， A_2 ， B_1 ， B_2 ， C_1 ， C_2 ）の値を操作する。

【0070】

埋込部30は、ここまで説明したように埋め込みデータが埋め込まれた輝度成分YのDCT係数（DCTブロック）と、クロマ成分 C_r ， C_b のDCT係数を、再びハフマン符号化して、JPEG方式により伸長可能な圧縮画像データ（JPEGデータ）として、画像DB24（図2）に対して出力する。

【0071】

〔埋込部30の構成部分〕

再び図3，4を参照して、埋込部30の構成部分を説明する。

【0072】

〔復号部300〕

復号部300（図3）は、制御部26（図2）の制御に従って、カメラIF104またはメモ리카ードIF106を介して供給されるJPEGデータをハフマン復号し、復号の結果として得られる3種類のDCT係数（DCTブロック）の内、2種類のクロマ成分 C_r ， C_b のDCT係数（DCTブロック）を、符号化部304に対して出力し、輝度成分YのDCT係数（DCTブロック）を、データ埋込部32に対して出力する。

【0073】

〔データ埋込部 32〕

データ埋込部 32 は、図 7～図 11 を参照して説明した埋め込みデータの埋め込み処理を行う。

以下、図 4 を参照して、データ埋込部 32 の各構成部分を説明する。

〔0074〕

〔画像分割部 320〕

画像分割部 320 は、復号部 300 から入力される輝度信号 Y の DCT 係数（DCT ブロック；図 7（A））を、図 7（B），（C）に示したペアに分割して、係数操作部 328 に対して出力する。

〔0075〕

〔乱数発生部 322〕

乱数発生部 322 は、鍵情報 DB 22（図 2）から入力される例えば 64 ビットの鍵を用いて、16 ビットの線形合同法により乱数を発生し、発生した乱数 R_N を位置決め部 324 およびスクランブル部 326 に対して出力する。

〔0076〕

〔位置決め部 324〕

位置決め部 324 は、画像分割部 320 が作成したペアそれぞれにおいて、乱数発生部 322 から入力される乱数 R_N を用いて、2 つの DCT ブロック（ブロック 1，2）のいずれの DCT 係数を選択するか（選択する DCT 係数の位置；図 8）を決定し、決定した DCT 係数の位置を示す位置データを係数操作部 328 に対して出力する。

〔0077〕

〔スクランブル部 326〕

スクランブル部 326 は、乱数発生部 322 から入力される乱数 R_N を用いて、埋込データ生成部 20（図 2）から入力される 96 ビットの埋め込みデータをスクランブル処理する。

このスクランブル部 326 のスクランブル処理により、96 ビットを 1 つの繰り返し単位とし、繰り返し単位ごとに異なった順番で 96 ビットの埋め込みデータの全てのビットを含み、この繰り返し単位を 64 個含むデータ（スクランブル

された埋め込みデータ、以下、単に埋め込みデータとも記す) を係数操作部 3 2 8 に対して出力する。

【0 0 7 8】

〔係数操作部 3 2 8 の埋め込みテーブル作成処理〕

係数操作部 3 2 8 は、まず、図 1 1 に示した埋め込みテーブルを作成する。

つまり、まず、係数操作部 3 2 8 は、位置決め部 3 2 4 から入力された位置データに基づいて、各ペアの 2 つの DCT ブロック (ブロック 1, 2 ; 図 7 (B) 等) から DCT 係数を取り出し (図 8)、埋め込みテーブル (図 1 1) のブロック 1, 2 の欄に書き込み、さらに、スクランブル部 3 2 6 から入力された埋め込みデータを埋め込みテーブルの埋め込みデータの割り当て欄に書き込む。

【0 0 7 9】

〔係数操作部 3 2 8 のデータ埋め込み処理〕

図 1 2 は、図 4 に示した係数操作部 3 2 8 が、DCT ブロックのペアに埋め込みデータを埋め込む処理 (S 1 0) を示す図である。

次に、係数操作部 3 2 8 は、DCT 係数 (DCT ブロック) のペアそれぞれに、埋め込みテーブル (図 1 1) において対応付けられた埋め込みデータのビットを埋め込み、埋め込みデータを埋め込んだ輝度成分の DCT 係数 Y' として符号化部 3 0 4 (図 3) に対して出力する。

【0 0 8 0】

図 1 2 に示すように、係数操作部 3 2 8 は、ステップ 1 0 0 (S 1 0 0) において、6 1 4 4 個のペアを示す変数 i を 1 に初期設定する。

【0 0 8 1】

ステップ 1 0 2 (S 1 0 2) において、係数操作部 3 2 8 は、第 i 番目のペアの操作対象となる DCT 係数 (A_1 , A_2 , B_1 , B_2 , C_1 , C_2) を、埋め込みテーブル (図 1 1) のブロック 1, 2 欄から、埋め込むビットを、同じく埋め込みテーブルの埋め込みデータ割り当て欄から取り出す。

【0 0 8 2】

ステップ 1 0 4 (S 1 0 4) において、係数操作部 3 2 8 は、S 1 0 2 の処理において取り出した埋め込みビットの値が 1 であるか否かを判断し、1 である場

合にはS106の処理に進み、これ以外の場合にはS110の処理に進む。

【0083】

ステップ106 (S106) において、係数操作部328は、操作対象のDCT係数が、表1に示した規則1-1または規則1-2を満たすか否かを判断し、図10に例示したように、規則1-1を満たす場合にはS114の処理に進み、図9(A)に例示したように、規則1-1も規則1-2も満たさない場合にはS108の処理に進む。

【0084】

ステップ108 (S108) において、係数操作部328は、操作対象のDCT係数が、規則1-1を満たすように操作する。

【0085】

ステップ110 (S110) において、係数操作部328は、操作対象のDCT係数が、表1に示した規則1-1または規則1-2を満たすか否かを判断し、規則1-2を満たす場合にはS114の処理に進み、規則1-1も規則1-2も満たさない場合にはS112の処理に進む。

【0086】

ステップ112 (S112) において、係数操作部328は、操作対象のDCT係数が、規則1-2を満たすように操作する。

【0087】

ステップ114 (S114) において、係数操作部328は、変数*i*が6144であるか否か、つまり、全てのペアに対して埋め込みデータの埋め込み処理が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数*i*を1増やしてS102の処理に戻る。

【0088】

[符号化部304]

符号化部304 (図3) は、復号部300から入力されたクロマ成分C_r、C_bのDCT係数と、データ埋込部32から入力され、埋め込みデータが埋め込まれた輝度成分YのDCT係数Y' とをハフマン符号化し、画像DB22に対して出力する。

【0089】

[抽出部40]

図13は、図2に示した抽出部40の構成を示す図である。

図14は、図13に示した埋め込みデータ抽出部42の構成を示す図である。

図13および図14に示すように、抽出部40は、復号部400、画像分割部402、符号化部404、画像合成部406、埋込データ抽出部42、改変検出部44およびクラスタリング部46から構成され、埋込データ抽出部42は、乱数生成部420、位置決め部422、抽出順序生成部424、対応付け部426およびデータ抽出部428から構成される。

【0090】

[抽出部40の概要]

埋込部30により、図7～図12を参照して上述したように埋め込みデータが埋め込まれたJPEGデータの一部または全部に対して、その後、改変が加えられると、各ペアの2つのDCTブロック（ブロック1，2；図7（B）等）の間で相互に対応し、埋め込みデータの埋め込みに用いられたDCT係数（ A_1 ， A_2 ， B_1 ， B_2 ， C_1 ， C_2 ；図8等）の値の関係が、上記表1に示した規則1-1，1-2に従って、図9（A），（B）および図10に例示した処理により埋め込まれたビットの値を示さなくなる。

【0091】

抽出部40は、上述した構成部分により、埋め込みデータが埋め込まれたJPEGデータのこのような性質を利用して、埋込部30が生成したJPEGデータに改変が加えられたか否か、および、改変が加えられた場合には、画像データ（図5）のいずれの部分に改変が加えられたかを判定し、表示する。

【0092】

[抽出部40の詳細]

以下、図15～図22をさらに参照して、抽出部40の処理を詳細に説明する。

上述したように、埋込部30（図2，3）においては、各ペアにおいて、埋め込みデータの埋め込みに用いられるDCT係数の位置は、同じく、鍵情報DB2

2から供給された鍵から生成された乱数によって求められる。

従って、抽出部40においても、埋込部30と同じ鍵を使うことにより、各ペアのDCTブロック（ブロック1，2；図8）において、いずれのDCT係数が、埋め込みデータの埋め込みに用いられたかを知ることができる。

【0093】

また、埋込部30においては、96ビットの埋め込みデータの各ビットは、鍵情報DB22から供給される鍵から生成された乱数によってスクランブルされ、各ペアに対応付けられている。

従って、抽出部40においても、埋込部30と同じ鍵を使うことにより、いずれのペアに、96ビットの埋め込みデータのいずれのビットが対応付けられたかを知ることができる。

【0094】

抽出部40は、このように、埋込部30と同じ鍵を用いて、各ペアの2つのDCTブロック（ブロック1，2）において、いずれのDCT係数がビットの埋め込みに用いられたかを知り、さらに、ビットの埋め込みに用いられた相互に対応するDCT係数同士の値の関係が、上記表1に示した規則1-1，1-2のいずれに該当するかによって、各ペアに埋め込まれた埋め込みデータのビットの値（1，0）を抽出する。

次に、抽出部40は、埋込部30と同じ鍵を用いて、各ペアから抽出された埋め込みデータのビットの値が、埋め込みデータのいずれのビットに対応するかを判定する。

【0095】

図15（A）は、埋込部30（図2，3）が埋め込みデータを埋め込んだJPEGデータを伸長した画像を例示する図であり、（B）は、（A）に示した画像に加えられた改変を例示する図であり、（C）は、改変後の画像を例示する図である。

ここで、例えば、埋込部30が、図5および図6（A）～（C）に示した画像データから得られたJPEGデータに対して、図7～図12に示したように埋め込みデータを埋め込んで生成したJPEGデータを、誰かが伸長し、図15（A

）に例示する画像を得て、図 15（B）に点線で示すように改変を加え、図 15（C）に示すように、画像左上の雲の部分消去した画像を生成し、再度、J P E G方式で圧縮符号化し、元の J P E Gデータと置き換えたとすると、改変は画像のごく一部に加えられたため、埋め込みデータの同一のビットに対応付けられた 64 個のペアから抽出された 64 の値の多くは、改変前の値を示し、少数だけが改変によって変更された値を示すはずである。

【0096】

抽出部 40 は、画像の一部に変更が加えられた場合のこのような性質を利用して、各ペアから抽出したビットを、埋め込みデータの各ビットに対応付けて多数決を採り、埋め込みデータの第 k ビットに対応する 64 個のペアの多数から値 1（0）が抽出され、少数のペアから値 0（1）が抽出された場合には、埋込部 30 が、これら 64 個のペアに、第 k ビットとして、値 1（0）を埋め込んだと推定する。

つまり、抽出部 40 は、埋め込みデータの各ビットについて、抽出された値の多数決を採り、埋込部 30 が各ペアに埋め込んだ埋め込みデータのビットの値を推定するとともに、多数決の結果、少数となった値が抽出されたペアに対して、改変が加えられたと判定する。

【0097】

図 16 は、改変が加えられた部分を示す 2 値画像を、元の画像と合成して示す画像を例示する図である。

さらに、抽出部 40 は、例えば、図 16 に示すように、改変が加えられたペアを示す 2 値画像（図 16 左上のモザイク状の部分）と、図 5 に示した元の画像とを合成して、いずれの部分に改変が加えられたかを表示装置 100（図 1）等に表示する。

【0098】

図 17 は、クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。

あるいは、抽出部 40 は、例えば、図 17 に示すように、クラスタリング処理により、図 16 に示した 2 値画像のモザイク状の部分が存在する範囲を示す画像

(図 1 7 左上の長方形)を得て、この画像と、図 5 に示した元の画像とを合成して、いずれの範囲に改変が加えられたかを表示装置 1 0 0 等に表示する。

【 0 0 9 9 】

このような処理を行うために、まず、抽出部 4 0 は、画像 DB 2 2 から供給される J P E G データをハフマン復号し、得られた 3 種類の D C T 係数 (D C T ブロック) の内、輝度成分 Y の 1 2 2 8 8 個の D C T 係数 (D C T ブロック Y') を取り出し、隣り合った D C T 同士を、図 7 (B) , (C) に示したように、6 1 4 4 個のペアにする。

【 0 1 0 0 】

抽出部 4 0 は、これらのペアそれぞれに含まれる 2 つの D C T ブロック (ブロック 1, 2 ; 図 8) の埋め込みデータの埋め込みに用いられた D C T 係数の関係が、上記表 1 に示した規則 1 - 1, 1 - 2 のいずれに該当するかを判断し、各ペアかに埋め込まれた埋め込みデータ (第 2 の埋め込みデータ) のビットの値 (1, 0) を抽出する。

もし、2 つの D C T ブロック (D C T ブロック 1, 2) の対応する D C T 係数が等しい場合 (例えば、 $A_1 = A_2$) には、この関係は規則 1 - 1, 1 - 2 のいずれにも当てはまらないため、抽出部 4 0 は、直ちにこのペアに改変が加えられたと判断することができる。以下、説明を明確化するために、対応する D C T 係数が等しくない場合を具体例とする。

【 0 1 0 1 】

図 1 8 は、埋込部 3 0 (図 2, 3) が生成した J P E G データに、改変・誤りが加えられていない場合に、抽出部 4 0 が改変等がなされていない J P E G データに含まれる各ペアから抽出するビットの値を示す図である。

抽出部 4 0 が、埋込部 3 0 が生成した後、改変も誤りも加えられていない J P E G データに含まれる各ペア (第 2 の画像ブロック) から抽出した埋め込みデータのビットの値を、図 1 8 に示すように、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、各埋め込みデータに対応するペアから抽出された全てのビットの値は一致する。

【 0 1 0 2 】

図 1 9 は、埋込部 3 0（図 2， 3）が生成した J P E G データに、改変・誤りが加えられた場合に、抽出部 4 0 が改変等がなされた J P E G データに含まれる各ペアから抽出するビットの値を例示する図である。

一方、例えば、抽出部 4 0 が、埋込部 3 0 が生成した後、改変等が加えられた J P E G データに含まれる各ペア（第 2 の画像ブロック）から抽出した埋め込みデータのビットの値を、図 1 8 と同様に、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、図 1 9 に示すように、改変が加えられた部分の少数のペアから抽出されたビットは、図 1 9 中に四角を付した値として示すように、改変が加えられていない他の多数のペアから抽出されたビットと異なる値を採る。

抽出部 4 0 は、このようにして多数決により得られたビットの値を、埋込部 3 0 が埋め込んだ埋め込みデータのビットの値と推定する。

【 0 1 0 3 】

図 2 0 は、抽出部 4 0（図 1 3， 1 4）が、図 1 5 に例示したように改変が加えられた J P E G データから、図 1 9 に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す 2 値画像を例示する図である。なお、説明の都合上、図 2 0 に示した例と、図 1 5 等 に示した例とは、必ずしも一致しない。

このように、抽出部 4 0 は、図 2 0 に例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれに位置するかを示す 2 値画像を生成する。

なお、抽出部 4 0 が生成した 2 値画像は、図 1 6 を参照して上述したように、元の画像と合成され、表示装置 1 0 0（図 1）等に表示される。

【 0 1 0 4 】

図 2 1（A）～（D）は、抽出部 4 0（図 1 3， 1 4）が、図 1 5 に例示したように改変が加えられた J P E G データから、図 1 9 に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。なお、説明の都合上、図 2 1（A）～（D）に示した例と、図 1 5 等 に示した例とは、必ずしも

一致しない。

また、抽出部 4 0 は、図 2 1 (A)，(C) にそれぞれ例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれの範囲に存在するかを判定し、それぞれ図 2 1 (B)，(D) に例示するクラスタリング画像を生成する。

なお、抽出部 4 0 が生成したクラスタリング画像は、図 1 7 を参照して上述したように、元の画像と合成され、表示装置 1 0 0 (図 1) 等に表示される。

【0 1 0 5】

〔抽出部 4 0 の構成部分〕

以下、再び図 1 3，1 4 を参照して、抽出部 4 0 の各構成部分を説明する。

【0 1 0 6】

〔復号部 4 0 0〕

復号部 4 0 0 は、操作に応じた制御部 2 6 に制御に従って、画像 DB 2 2 から供給される J P E G データをハフマン復号し、復号の結果として得られた 3 種類の画像成分の内、クロマ成分 C r，C b を符号化部 4 0 4 に対して出力し、輝度成分 Y' を、画像分割部 4 0 2 に対して出力する。

【0 1 0 7】

〔画像分割部 4 0 2〕

画像分割部 4 0 2 は、復号部 4 0 0 から入力された輝度成分 Y' を、D C T 係数 (D C T ブロック) 単位に分割し、分割の結果として得られた D C T 係数 (D C T ブロック) を、埋込データ抽出部 4 2 に対して出力する。

【0 1 0 8】

〔埋込データ抽出部 4 2〕

埋込データ抽出部 4 2 は、画像分割部 4 0 2 から入力された輝度成分 Y' の D C T ブロックを 2 つずつ対応付けて、埋込部 3 0 においてと同様なペア (図 7 (B)，(C) および図 8 等) とし、これらのペアに埋め込まれた埋め込みデータのビットの値を抽出し、図 1 8，1 9 に例示した形式の抽出データとして改変検出部 4 4 に対して出力する。

また、埋込データ抽出部 4 2 は、画像分割部 4 0 2 から入力された輝度成分 Y

をそのまま、輝度成分 Y として符号化部 404 に対して出力する。

【0109】

〔対応付部 426〕

対応付部 426 (図 14) は、画像分割部 402 から入力された 12288 個の DCT 係数 (DCT ブロック) の内、隣り合った 2 つの DCT ブロック (ブロック 1, 2 ; 図 7 (B) 等) 同士を対応付け、6144 個の DCT 係数のペア (図 7 (B), (C)) を生成し、データ抽出部 428 に対して出力する。

つまり、対応付部 426 は、埋込部 30 (図 2, 3) の画像分割部 320 (図 4) に対応し、画像分割部 320 と同様に、DCT ブロックのペアを生成する。

【0110】

〔乱数発生部 420〕

乱数発生部 420 は、鍵情報 DB 22 (図 2) から供給され、埋込部 30 が埋め込みデータの埋め込みに用いた鍵と同じ鍵を用いて、埋込部 30 においてと同じ方法により乱数 RN を発生し、発生した乱数 RN を、位置決め部 422 および抽出順序生成部 424 に対して出力する。

つまり、乱数発生部 420 は、埋込部 30 の乱数発生部 322 (図 4) に対応し、乱数発生部 322 が用いる鍵と同一の鍵から、乱数発生部 322 と同一方法で同一の乱数を生成する。

【0111】

〔位置決め部 422〕

位置決め部 422 は、乱数発生部 420 から入力された乱数 RN から、ペアそれぞれに含まれる 2 つの DCT ブロック (ブロック 1, 2) のいずれの DCT 係数が、埋込部 30 において埋め込みデータの埋め込みに用いられたかを示す位置データを生成し、データ抽出部 428 に対して出力する。

つまり、位置決め部 422 は、埋込部 30 の位置決め部 324 に対応し、位置決め部 324 が用いた乱数と同一の乱数から、位置決め部 324 と同一の位置データを生成する。

【0112】

〔抽出順序生成部 424〕

上述したように、対応付部 426 からデータ抽出部 428 に入力される 6144 個のペアは、96 個のペアを 1 組として、各組ごとに異なる順番で、各組に含まれる 96 個のペアそれぞれに、96 ビットの埋め込みデータのビットそれぞれが対応付けられている。

抽出順序生成部 424 は、乱数発生部 420 から入力された乱数 RN から、いずれのペアに、96 ビットの埋め込みデータのいずれの順番のビットが対応付けられたかを示す順序データを生成し、データ抽出部 428 に対して出力する。

【0113】

データ抽出部 428 は、対応付部 426 から入力されるペアそれぞれに含まれる 2 つの DCT ブロック（ブロック 1，2）において、位置決め部 422 から入力される位置データが示す相互に対応する DCT 係数（図 8 等）同士の値の関係が、上記表 1 に示した規則 1-1，1-2 のいずれと一致するかを判定し、各ペアに埋め込まれた埋め込みデータのビットの値を抽出する。

さらに、データ抽出部 428 は、抽出したビットの値を、抽出順序生成部 424 から入力される順序に従って並び替え、図 18，19 に例示した形式の抽出データを生成し、抽出順序生成部 424 に対して出力する。

【0114】

データ抽出部 428 のビット抽出処理を、図 22 を参照してさらに説明する。

図 22 は、図 14 に示したデータ抽出部 428 が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。

図 22 に示すように、ステップ 120（S120）において、データ抽出部 428 は、6144 個のペアを示す変数 i に 1 を代入し、初期設定を行う。

【0115】

ステップ 122（S122）において、データ抽出部 428 は、変数 i が示す第 i 番目のペアを抽出対象として取り出す。

【0116】

ステップ 124（S124）において、データ抽出部 428 は、取り出した抽出対象のペアに含まれる 2 つの DCT ブロック（ブロック 1，2）において、位置決め部 422 から入力される位置データが示す DCT 係数の関係が、上記表 1

に示した規則 1-1, 1-2 のいずれに当てはまるかを判定し、規則 1-1 に当てはまる場合には、第 i 番目のペアから値 1 のビットを抽出し、規則 1-2 に当てはまる場合には、値 0 のビットを抽出する。

さらに、データ抽出部 428 は、抽出順序生成部 424 から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ（図 18, 19）中の判定の結果として得られた位置に、抽出したビットの値（1, 0）を書き込む。

【0117】

ステップ 126（S126）において、データ抽出部 428 は、変数 i が 6144 であるか否か、つまり、全てのペアからのビットの抽出が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数 i を 1 増やして S122 の処理に進む。

【0118】

全てのペアからビットの抽出が完了すると、データ抽出部 428 は、図 18, 19 に例示した抽出データにおいて、96 ビットの埋め込みデータのビットそれぞれに対応して抽出された 64 個の値の多数決を採り、埋込部 30（図 2, 3）において埋め込まれた埋め込みデータを推定し、各ペアを輝度成分 Y として符号化部 404 に対して出力する。

【0119】

〔符号化部 404〕

符号化部 404（図 13）は、復号部 400 から入力されたクロマ成分 C_r , C_b および符号化部 404 から入力された輝度成分 Y をハフマン符号化して、JPEG データを生成し、画像合成部 406 に対して出力する。

【0120】

〔改変検出部 44〕

改変検出部 44 は、データ抽出部 428 から入力された抽出データ（図 18, 19）から、図 20 に示した 2 値画像を生成し、画像合成部 406 に対して出力する。

【0121】

〔クラスタリング部 46〕

クラスタリング部 46 は、改変検出部 44 から入力された 2 値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像（図 21）を生成し、画像合成部 406 に対して出力する。

【0122】

〔画像合成部 406〕

画像合成部 406 は、操作入力に応じた制御部 26 の制御に従って、符号化部 404 から入力される J P E G データを伸長し、図 5 あるいは図 15（C）等に例示した画像を生成し、生成した画像をそのまま表示装置 100（図 1）に表示する。

あるいは、画像合成部 406 は、改変検出部 44 から入力された 2 値画像、あるいは、クラスタリング部 46 から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、図 16 あるいは図 17 に例示した画像を生成し、画像中において改変等がなされた部分を表示装置 100 に表示する。

あるいは、画像合成部 406 は、改変検出部 44 から入力された 2 値画像、あるいは、クラスタリング部 46 から入力されたクラスタリング画像を、そのまま表示装置 100 に表示して、画像中のいずれの範囲に改変等がなされたかを示す。

【0123】

〔画像改変判定装置 1 の埋め込みデータ埋め込み処理〕

以下、図 23 を参照して、画像改変判定装置 1 による埋め込みデータの埋め込み処理を、全体を通して説明する。

図 23 は、図 1 に示した画像改変判定装置 1 による埋め込みデータの埋め込み処理（S20）を示すフローチャートである。

【0124】

ステップ 200（S200）において、復号部 300（図 3）は、カメラ I F 104 等を介して供給される J P E G データをハフマン復号し、輝度成分 Y の 12288 個の D C T 係数（D C T ブロック）を、データ埋込部 32 に対して出力する。

画像分割部 320 は、入力された DCT 係数 (DCT ブロック ; 図 7 (A)) を、6144 個のペア (図 7 (B), (C)) に分割して、係数操作部 328 に対して出力する。

乱数発生部 322 は、鍵情報 DB 22 (図 2) から入力される鍵を用いて乱数を発生し、発生した乱数 RN を位置決め部 324 およびスクランブル部 326 に対して出力する。

【0125】

位置決め部 324 は、乱数発生部 322 から入力される乱数 RN を用いて、埋め込みデータの埋め込みに用いられる DCT 係数の位置を示す位置データを生成し、係数操作部 328 に対して出力する。

スクランブル部 326 は、乱数発生部 322 から入力される乱数 RN を用いて、埋込データ生成部 20 (図 2) から入力される 96 ビットの埋め込みデータをスクランブル処理し、係数操作部 328 に対して出力する。

【0126】

ステップ 12 (S12) において、まず、係数操作部 328 (図 4) は、各ペアにおいて、埋め込みデータを埋め込むための操作の対象となる DCT 係数 (A_1 , A_2 , B_1 , B_2 , C_1 , C_2 ; 図 8 等) を、位置決め部 324 から入力される位置データに基づいて選択する。

さらに、係数操作部 328 は、各ペアを、スクランブル部 326 から入力される埋め込みデータの各ビットと対応付け、図 11 に示した埋め込みテーブルを作成する。

さらに、係数操作部 328 は、埋め込みテーブルから操作の対象となる DCT 係数と、埋め込むビットとを順次、取り出し、上記表 1 に示した規則 1-1, 1-2 に従って、図 9 (A), (B) および図 10 に例示したように、各ペアに埋め込みデータの各ビットを埋め込む。

【0127】

全てのペアへのビットの埋め込みが終了すると、ステップ 202 (S202) において、符号化部 304 (図 3) は、埋め込みデータが埋め込まれた輝度成分の DCT 係数 (DCT ブロック) と、復号部 300 から入力されるその他の成分

のDCT係数とをハフマン符号化し、J P E Gデータを生成して画像DB 2 2（図2）に対して出力する。

画像DB 2 2は、埋込部30から入力されたJ P E Gデータを記憶・管理する。

【0128】

[画像改変判定装置1の埋め込みデータ抽出処理]

以下、図24を参照して、画像改変判定装置1による埋め込みデータの抽出処理を、全体を通して説明する。

図24は、図1に示した画像改変判定装置1による埋め込みデータの抽出処理（S22）を示すフローチャートである。

【0129】

ステップ220（S220）において、復号部400（図13）は、画像DB 2 2から供給されるJ P E Gデータをハフマン復号し、輝度成分Y'を、画像分割部402に対して出力する。

画像分割部402は、輝度成分Y'を12288個のDCT係数（DCTブロック）に分割して、埋込データ抽出部42に対して出力する。

埋込データ抽出部42において、対応付部426は、隣り合ったDCT係数（DCTブロック；図7（A））を2つずつ対応付けて、6144個のペア（図7（B），（C））を作成し、データ抽出部428に対して出力する。

乱数発生部420（図14）は、鍵情報DB 2 2（図2）から入力される鍵を用いて乱数を発生し、発生した乱数RNを位置決め部422および抽出順序生成部424に対して出力する。

【0130】

位置決め部422は、乱数発生部420から入力される乱数RNを用いて、埋め込みデータの埋め込みに用いられるDCT係数の位置を示す位置データを生成し、データ抽出部428に対して出力する。

抽出順序生成部424は、乱数発生部322から入力される乱数RNを用いて、各ペアに、いずれの埋め込みデータのビットが対応付けられているかを示す順序データを生成し、データ抽出部428に対して出力する。

【0131】

ステップ12 (S12) において、図22に示したように、データ抽出部428は、ペアを順次、取り出して抽出対象とし、位置決め部422から入力される位置データが示す2つのDCTブロック（ブロック1，2）のDCT係数の値の関係が、上記表1に示した規則1-1，1-2のいずれに当てはまるかに応じて、各ペアに埋め込まれたビットの値を抽出する。

さらに、データ抽出部428は、抽出順序生成部424から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ（図18，19）中の判定の結果として得られた位置に、抽出したビットの値（1，0）を書き込む。

【0132】

全てのペアからのビットの値の抽出が終了すると、ステップ222 (S222) において、データ抽出部428は、図18，19に例示した抽出データにおいて、96ビットの埋め込みデータのビットそれぞれに対応して抽出された64個の値の多数決を採り、埋込部30（図2，3）において埋め込まれた埋め込みデータを推定する。

さらに、符号化部404（図13）は、復号部400から入力されたクロマ成分Cr，Cbおよび符号化部404から入力された輝度成分Yをハフマン符号化して、JPEGデータを生成し、画像合成部406に対して出力する。

【0133】

ステップ224 (S224) において、改変検出部44は、データ抽出部428から入力された抽出データ（図18，19）から、図20に示した2値画像を生成し、画像合成部406に対して出力する。

クラスタリング部46は、改変検出部44から入力された2値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像（図21）を生成し、画像合成部406に対して出力する。

画像合成部406は、操作入力に応じた制御部26の制御に従って、例えば、改変検出部44から入力された2値画像、あるいは、クラスタリング部46から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、

図 16 あるいは図 17 に例示した画像を生成し、画像中において改変等がなされた部分を表示装置 100 に表示する。

【0134】

〔変形例〕

ここまで説明した実施形態においては、画像データの圧縮符号化のために DCT 処理を行う場合について説明したが、本発明にかかる改変判定方法は、DCT 処理ではなく、例えばウェーブレット変換、フーリエ変換および FFT（高速フーリエ変換）といった、空間領域のデータを周波数領域のデータに変換する空間・周波数変換を用いて画像データを圧縮符号化する場合にも、ほとんど変更なしに適用することができる。

また、実施形態においては、輝度成分 Y の DCT 係数に埋め込みデータを埋め込む場合を説明したが、本発明にかかる改変判定方法は、クロマ成分 C_r 、 C_b に埋込データを埋め込む場合にも応用可能である。

【0135】

また、実施形態においては、DCT ブロックの対応付けを、隣接した 2 つの DCT ブロック同士を対応付けることにより行ったが、例えば、乱数を用いて、12288 個の DCT ブロックの 2 つをランダムに選択し、対応付けしてペアとしてもよい。

また、図 4 に点線で示したように、乱数発生部 322 から画像分割部 320 に乱数 RN を供給し、画像分割部 320 が、この乱数 RN を用いて、ランダムに 2 つずつ DCT 係数（DCT ブロック）を選択してペアを作成するようにしてもよい。

【0136】

また、図 1.4 に点線で示したように、乱数発生部 420 から対応付部 426 に乱数 RN を供給し、対応付部 426 が、この乱数 RN を用いて、画像分割部 320 が対応付けたペアを再現するようにしてもよい。

また、埋込データのスクランブル方法は、実施形態として示した方法に限定されず、96 ビットの埋込データの各ビットが、6144 のペアに対して 64 回ずつ割り当てられるような方法であればよい。

【0137】

また、本発明にかかる埋込・判定プログラム2を適切に変形することにより、画像データの他、音声データ等、他の種類のコンテンツデータのいずれの部分に加えられたかを判定する用途に応用することができる。

音声データに対して本発明を応用する場合を例としてさらに説明する。

音声データは、連続するサンプル点を1ブロックとして処理することができ、例えば、サンプリング周波数44.1kHzの音声データ、1024個ずつを1つのブロックとすれば、1秒分の音声データには、44個の音声データブロックが含まれることになる。

これらの音声データブロックをFFTなどにより周波数領域のデータブロックに変換すると、実施形態と同様な方法により埋込データを埋め込むことができ、埋め込んだデータを用いて改変を検出することができる。

【0138】

図25は、それぞれ画像DB24(24-1~24-n)を有する複数の画像改変判定装置1(1-1~1-n)を接続した改変判定システム4の構成を示す図である。

なお、図25に示すように、それぞれ画像DB24(24-1~24-n)および埋込・抽出部3(3-1~3-n)を1つずつ含む複数の画像改変判定装置1-1~1-nを、通信装置116(図1;図25において図示せず)を介して接続して、各画像改変判定装置1-1~1-nで画像データに加えられた改変を検出する場合には、各画像DB24-1~24-nにおいて記憶・管理される画像データと、その鍵とを、画像改変判定装置1-1の鍵情報DB22-1により一元管理し、各画像改変判定装置1-1~1-nに対して鍵を配送すると、高いセキュリティを確保することができる。

【0139】

【発明の効果】

以上説明したように、本発明にかかる改変判定装置およびその方法によれば、単にコンテンツデータに対して改変が加えられているか否かを判定することができるだけでなく、さらに、コンテンツデータのいずれの部分に改変が加えられて

いるかまでを判定することができる。

【図面の簡単な説明】

【図 1】

本発明にかかる改変判定方法を実現する画像改変判定装置の構成を示す図である。

【図 2】

図 1 に示した画像改変判定装置が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラムの構成を示す図である。

【図 3】

図 2 に示した埋込部 3 0 の構成を示す図である。

【図 4】

図 3 に示したデータ埋込部 3 2 の構成を示す図である。

【図 5】

デジタルカメラ（図 1）が撮影した非圧縮画像データを例示する図である。

【図 6】

（A）は、図 5 に例示した非圧縮画像データの一部を示す図であり、（B）は、（A）に例示した非圧縮画像データ（部分）に含まれる D C T ブロック（マクロブロック）を示す図であり、（C）は、（B）に示した D C T ブロックそれぞれに含まれる 8 画素×8 画素構成の画素を示す図である。

【図 7】

（A）は、デジタルカメラから入力される非圧縮画像データを復号部がハフマン復号して得られる輝度信号 Y の D C T 係数を示す図であり、（B）は、（A）に示した輝度信号 Y の D C T 係数の内、それぞれ隣り合う 2 組を対応付ける方法を示す図であり、（C）は、（B）に示した方法により対応付けられた D C T 係数のペアを示す図である。

【図 8】

図 2、3 に示した埋込部が 1 つのペア（図 7（A），（B））に含まれる D C T ブロック（ブロック 1，2）それぞれから選択した相互に対応する D C T 係数を例示する図である。

【図 9】

(A), (B) は、図 8 に例示したように選択されたブロック 1, 2 それぞれの DCT 係数を、埋め込みデータのビット (値 1) を埋め込むために、DCT 係数の数値を変更する必要がある場合について例示する図である。

【図 1 0】

図 8 に例示したように選択されたブロック 1, 2 それぞれの DCT 係数を、埋め込みデータのビット (値 1) を埋め込むために、DCT 係数の数値を変更する必要がない場合について例示する図である。

【図 1 1】

埋込部 (図 2, 3) が、DCT ブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。

【図 1 2】

図 4 に示した係数操作部が、DCT ブロックのペアに埋め込みデータを埋め込む処理 (S 1 0) を示す図である。

【図 1 3】

図 2 に示した抽出部の構成を示す図である。

【図 1 4】

図 1 3 に示した埋め込みデータ抽出部の構成を示す図である。

【図 1 5】

(A) は、埋込部 (図 2, 3) が埋め込みデータを埋め込んだ J P E G データを伸長した画像を例示する図であり、(B) は、(A) に示した画像に加えられた改変を例示する図であり、(C) は、改変後の画像を例示する図である。

【図 1 6】

改変が加えられた部分を示す 2 値画像を、元の画像と合成して示す画像を例示する図である。

【図 1 7】

クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。

【図 1 8】

埋込部（図 2， 3）が生成した J P E G データに、改変・誤りが加えられていない場合に、抽出部が改変等がなされていない J P E G データに含まれる各ペアから抽出するビットの値を示す図である。

【図 19】

埋込部（図 2， 3）が生成した J P E G データに、改変・誤りが加えられた場合に、抽出部が改変等がなされた J P E G データに含まれる各ペアから抽出するビットの値を例示する図である。

【図 20】

抽出部（図 13， 14）が、図 15 に例示したように改変が加えられた J P E G データから、図 19 に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す 2 値画像を例示する図である。

【図 21】

(A) ～ (D) は、抽出部（図 13， 14）が、図 15 に例示したように改変が加えられた J P E G データから、図 19 に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。

【図 22】

図 14 に示したデータ抽出部が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。

【図 23】

図 1 に示した画像改変判定装置による埋め込みデータの埋め込み処理（S 20）を示すフローチャートである。

【図 24】

図 1 に示した画像改変判定装置による埋め込みデータの抽出処理（S 22）を示すフローチャートである。

【図 25】

それぞれ画像 DB を有する複数の画像改変判定装置を接続した改変判定システムの構成を示す図である。

【符号の説明】

1, 1-1~1-n・・・画像改変判定装置

100・・・表示装置

102・・・入力装置

104・・・カメラ I F

106・・・メモリカード I F

108・・・記憶装置

110・・・PC本体

112・・・メモリ

114・・・CPU

116・・・通信装置

120・・・記録媒体

140・・・デジタルカメラ

142・・・メモリカード

2・・・埋込・判定プログラム

3, 3-1~3-n・・・埋込・抽出部

20・・・埋込データ生成部

22, 22-1・・・鍵情報DB

24, 24-1~24-n・・・画像DB

26・・・制御部

30・・・埋込部

300・・・復号部

32・・・データ埋込部

320・・・画像分割部

322・・・乱数発生部

324・・・位置決め部

326・・・スクランブル部

328・・・係数操作部

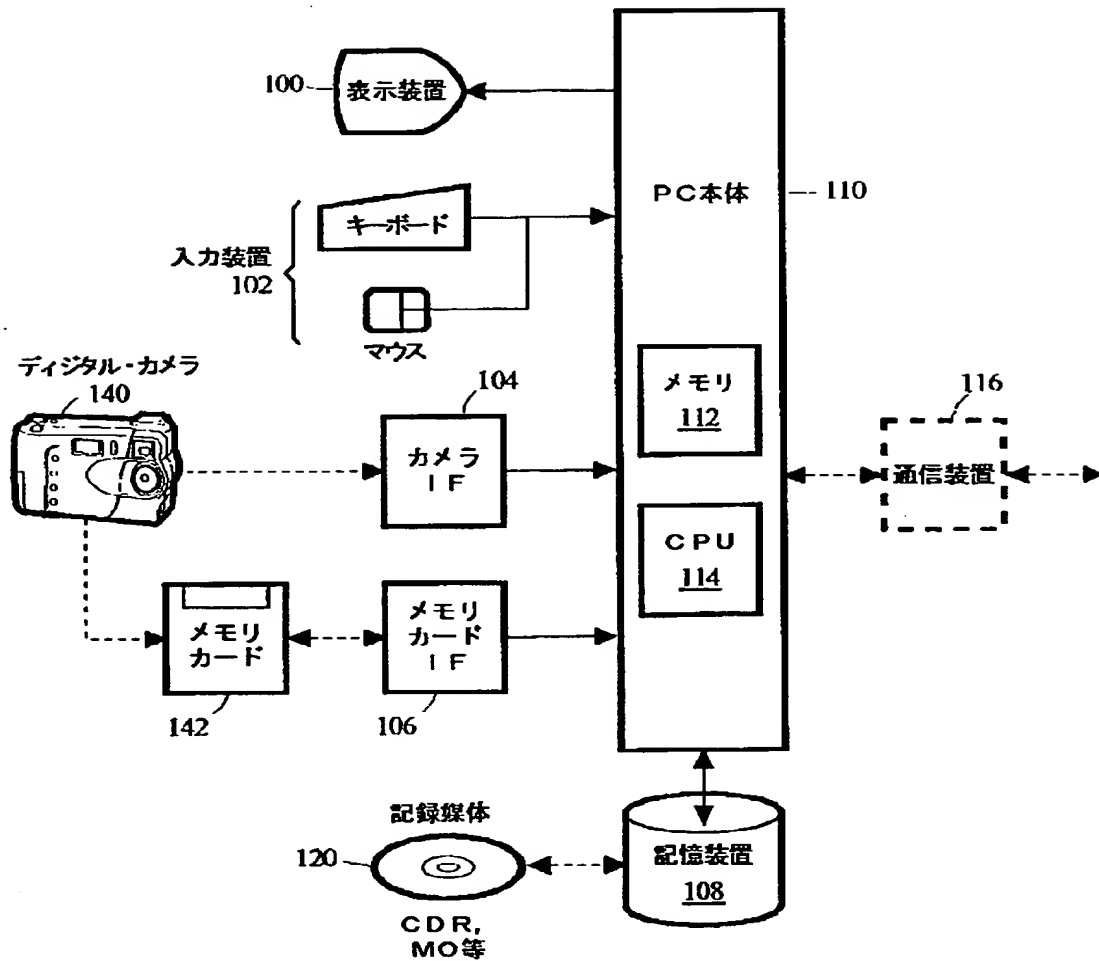
304・・・符号化部

40・・・抽出部

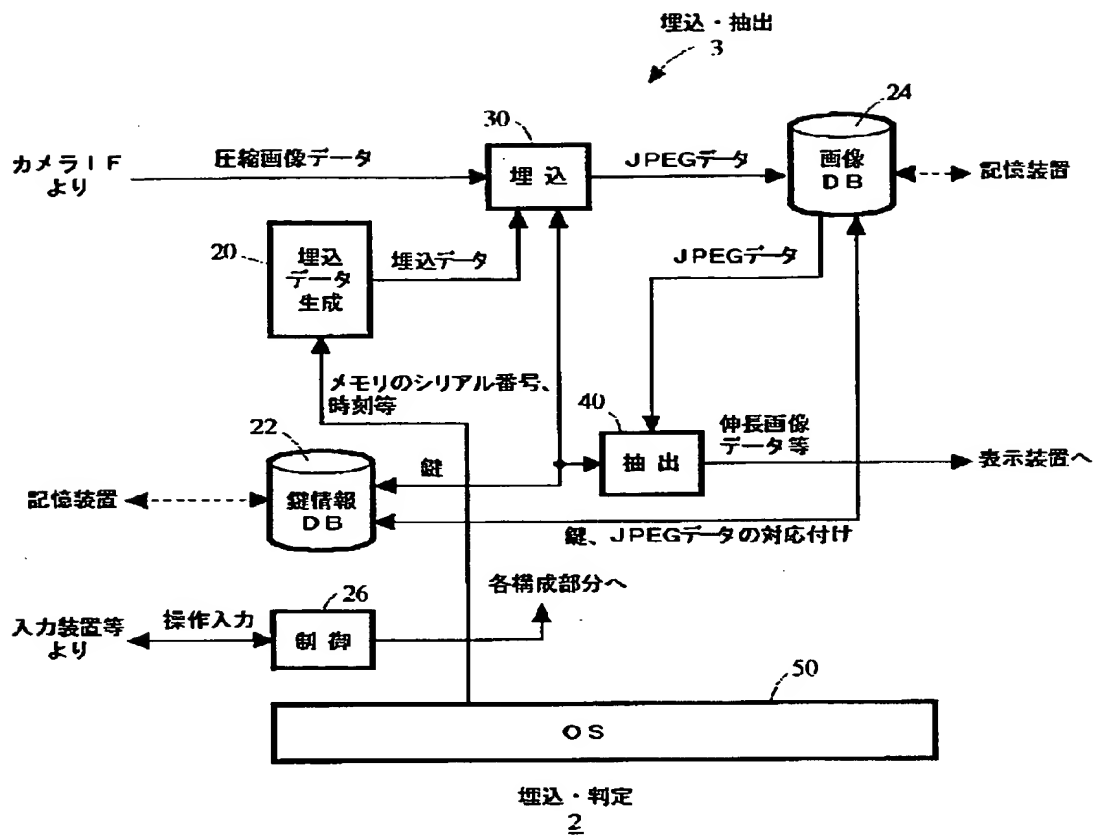
400 . . . 復号部
402 . . . 画像分割部
404 . . . 符号化部
406 . . . 画像合成部
42 . . . 埋込データ抽出部
 420 . . . 乱数発生部
 422 . . . 位置決め部
 424 . . . 抽出順序生成部
 426 . . . 対応付部
 428 . . . データ抽出部
44 . . . 改変検出部
46 . . . クラスタリング部
50 . . . OS

【書類名】 図面

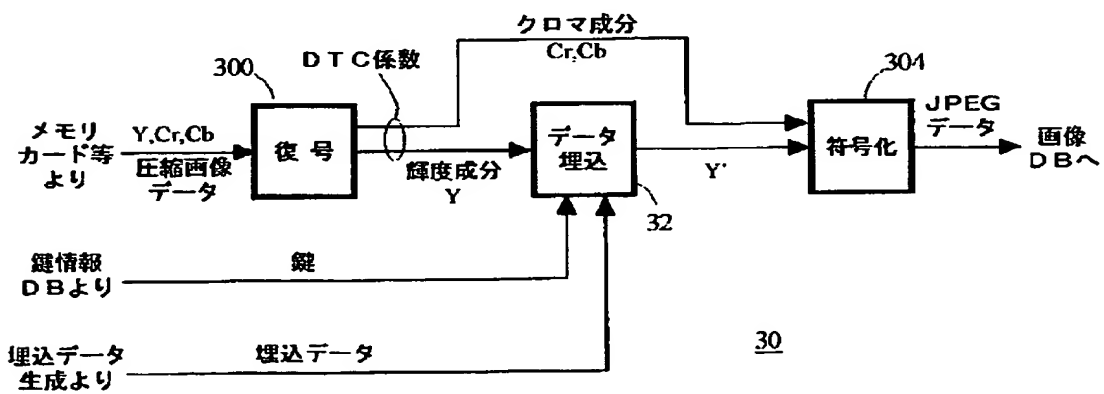
【図 1】



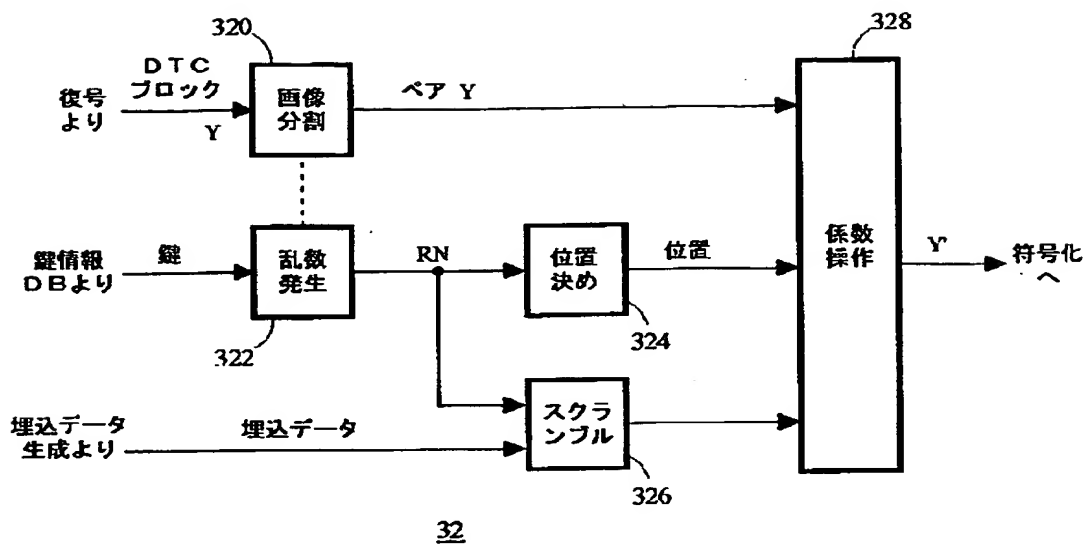
【図 2】



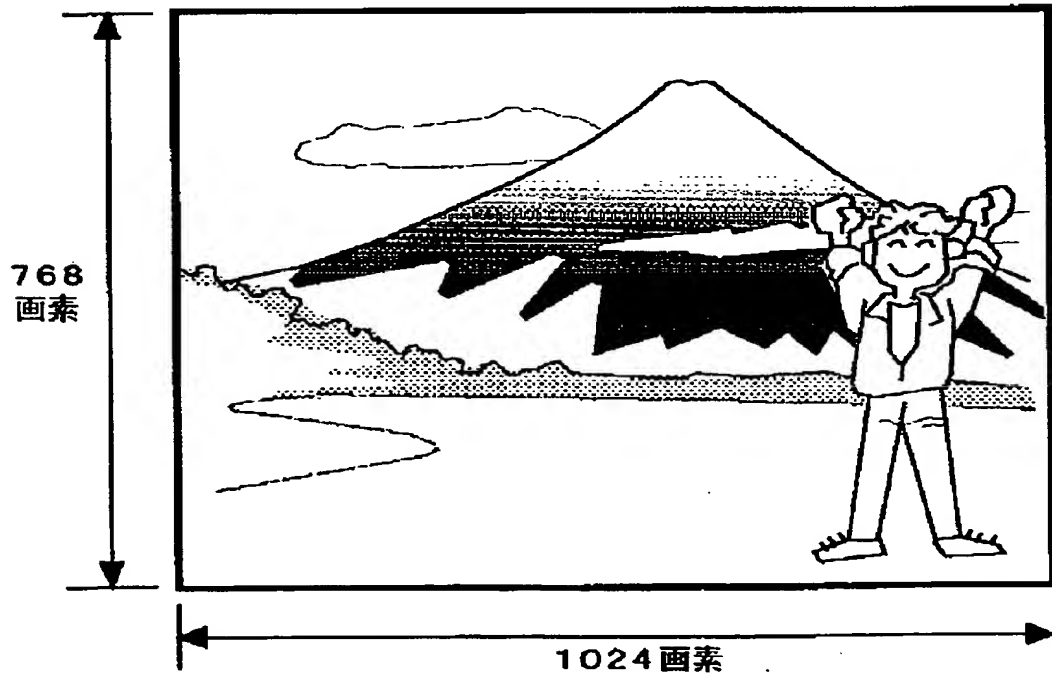
【図 3】



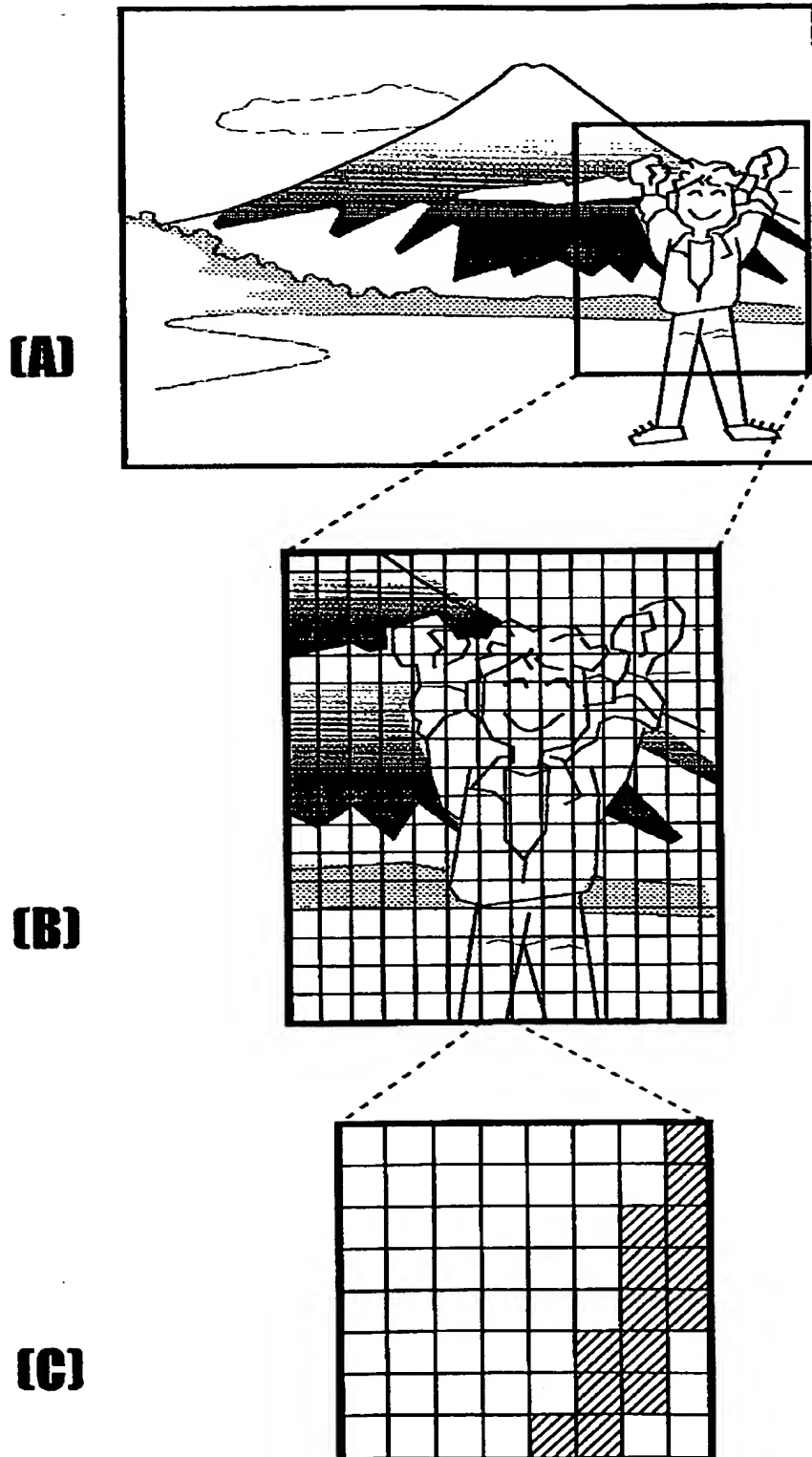
【図 4】



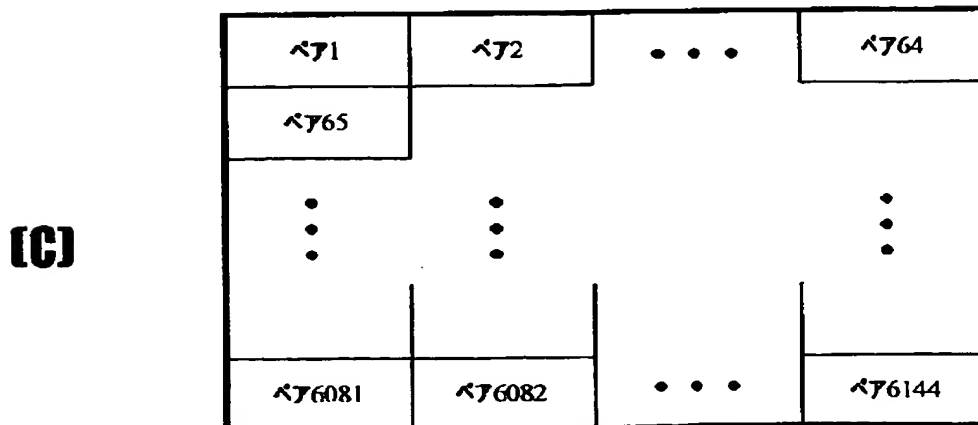
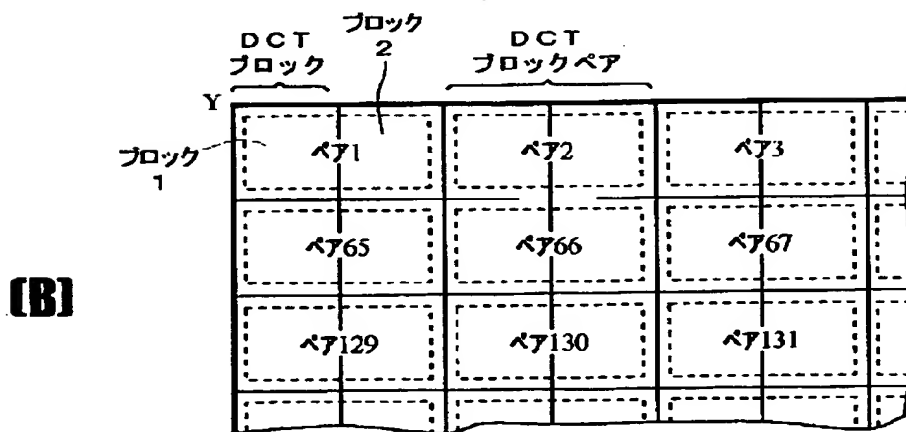
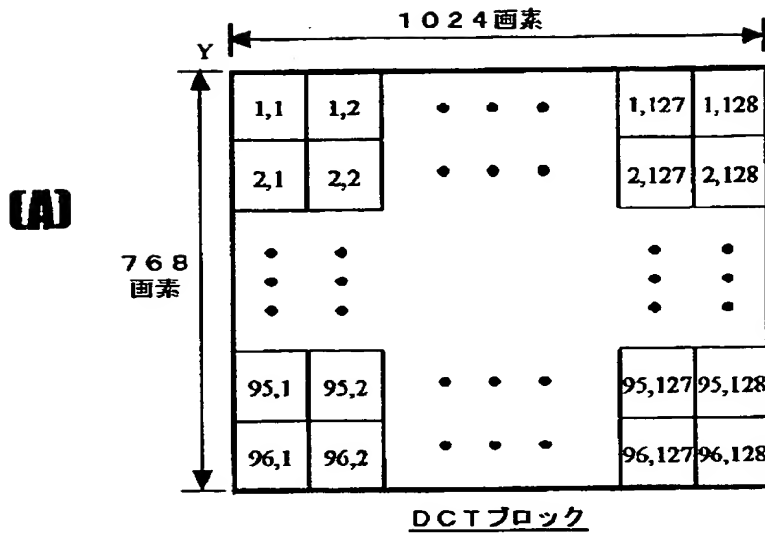
【図 5】



【図 6】

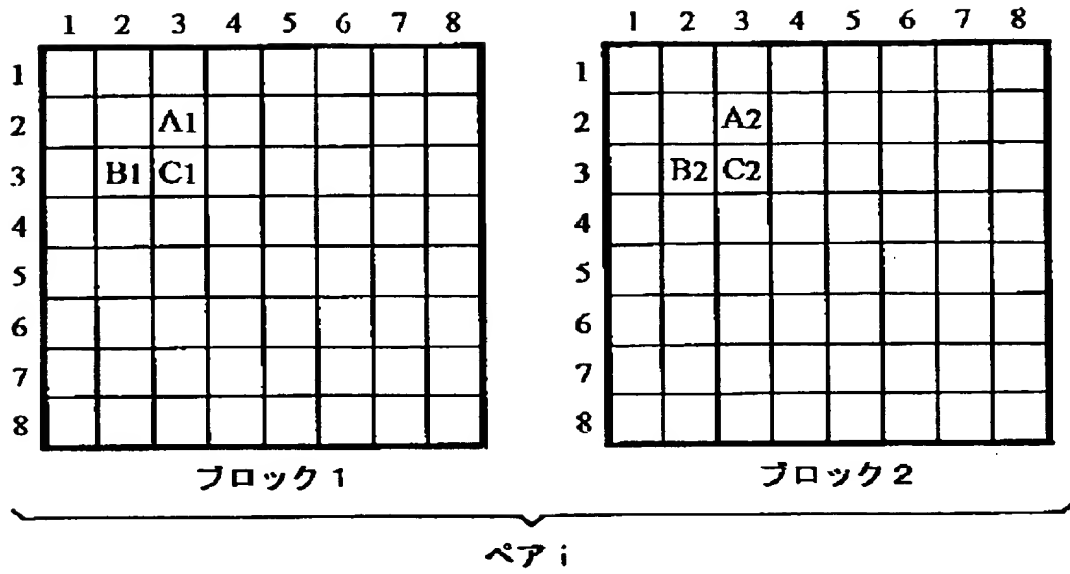


【図 7】



ベア

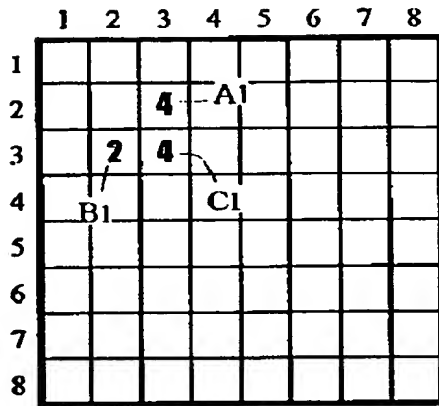
【図 8】



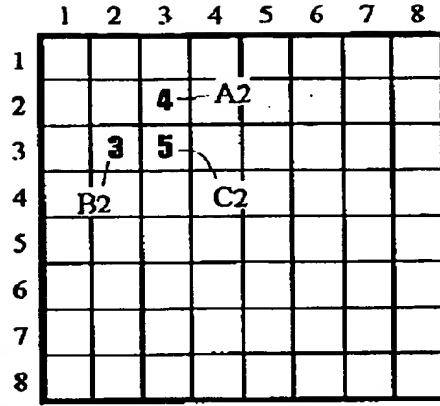
【図9】

ペア: ← ビット "1" を埋込む

(A)



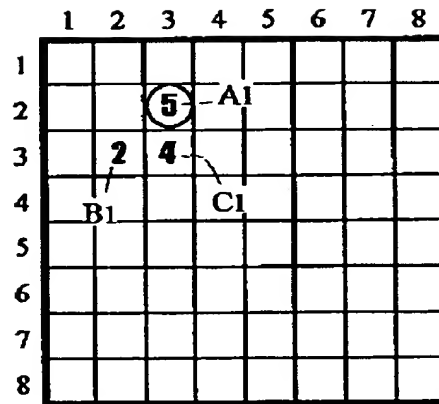
ブロック 1



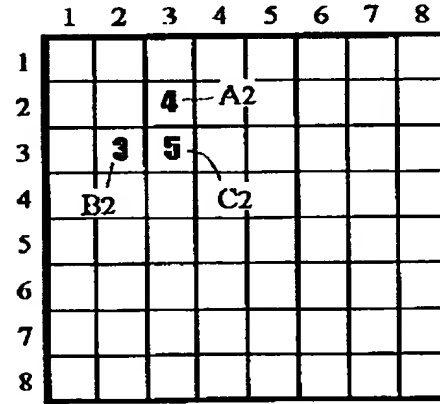
ブロック 2



(B)



ブロック 1



ブロック 2

【図 10】

ペア i ← ビット "1" を埋込む

	1	2	3	4	5	6	7	8
1								
2			3	A1				
3		6	5					
4		B1		C1				
5								
6								
7								
8								

ブロック 1

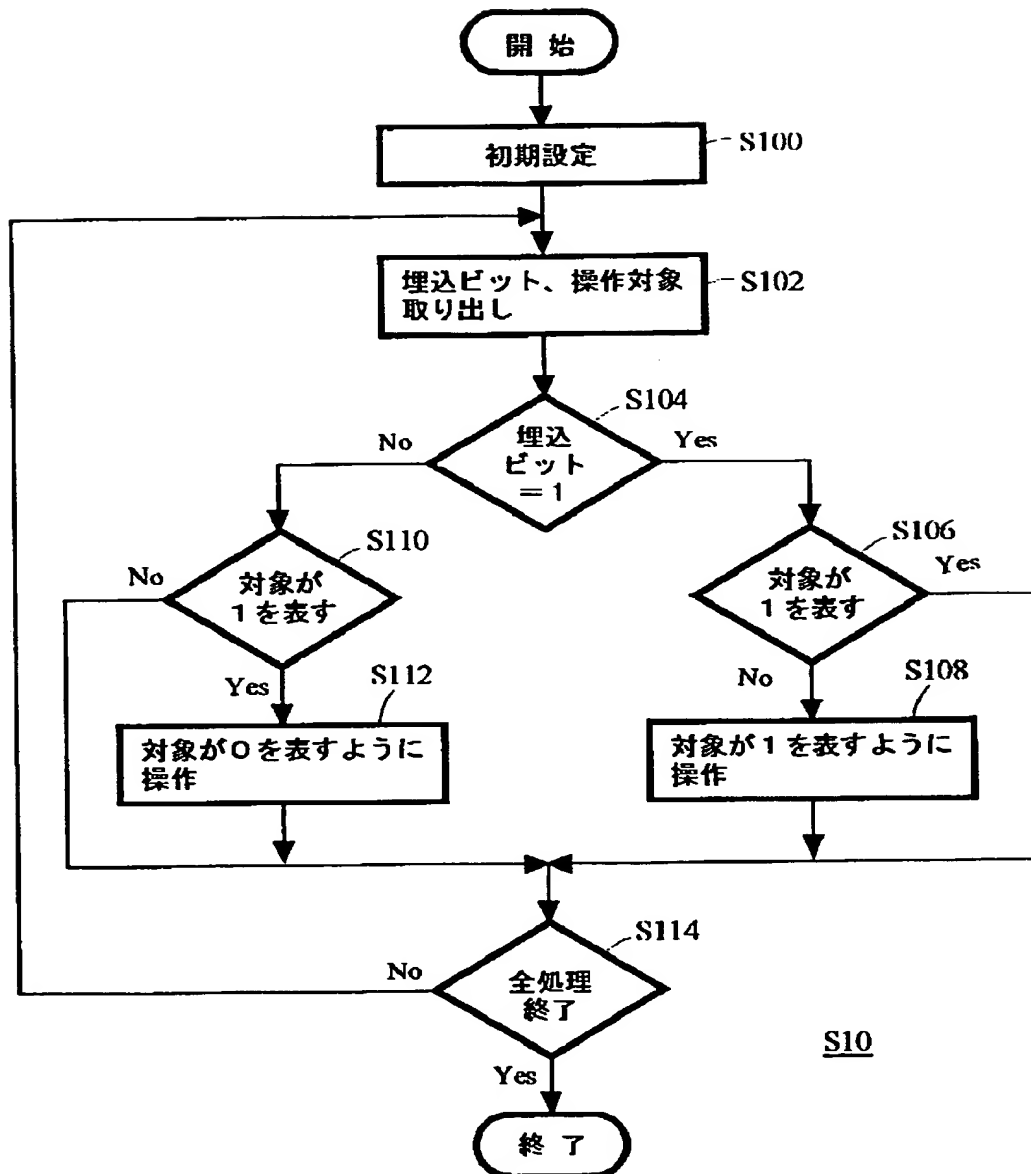
	1	2	3	4	5	6	7	8
1								
2			5	A2				
3		3	4					
4		B2		C2				
5								
6								
7								
8								

ブロック 2

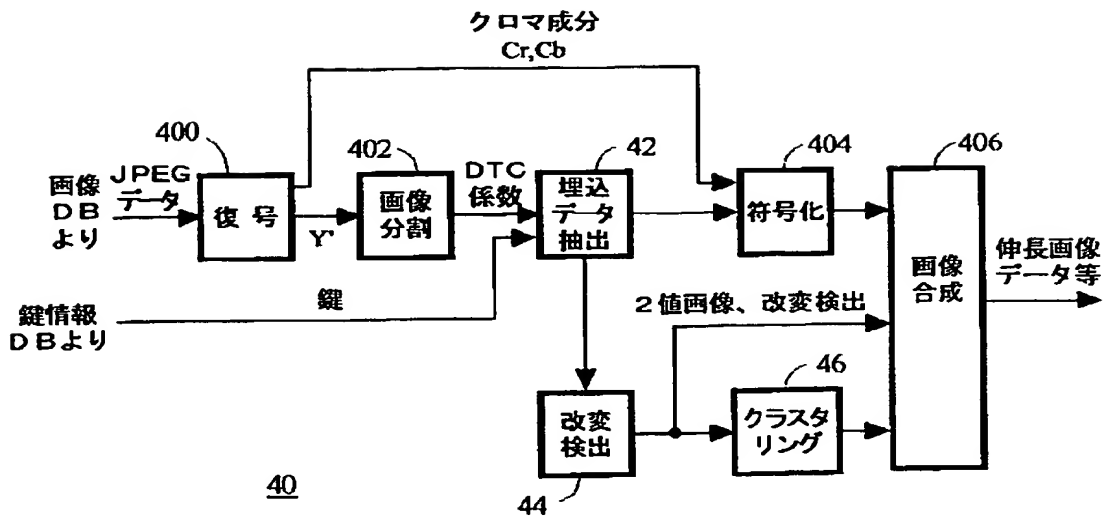
【図 11】

DCTブロック ペア番号	ブロック 1 係数			ブロック 2 係数			埋込データ ビット番号	埋込データ 割当て
	A1	B1	C1	A2	B2	C2	(1~96)	
1	1	5	2	5	6	3	31	1
2	5	8	9	2	5	5	21	0
3	2	10	9	5	1	2	18	1
4	1	11	5	5	3	20	65	0
5	10	2	25	1	3	24	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
160	5	30	11	6	9	10	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
6144	51	20	11	3	19	15	34	1

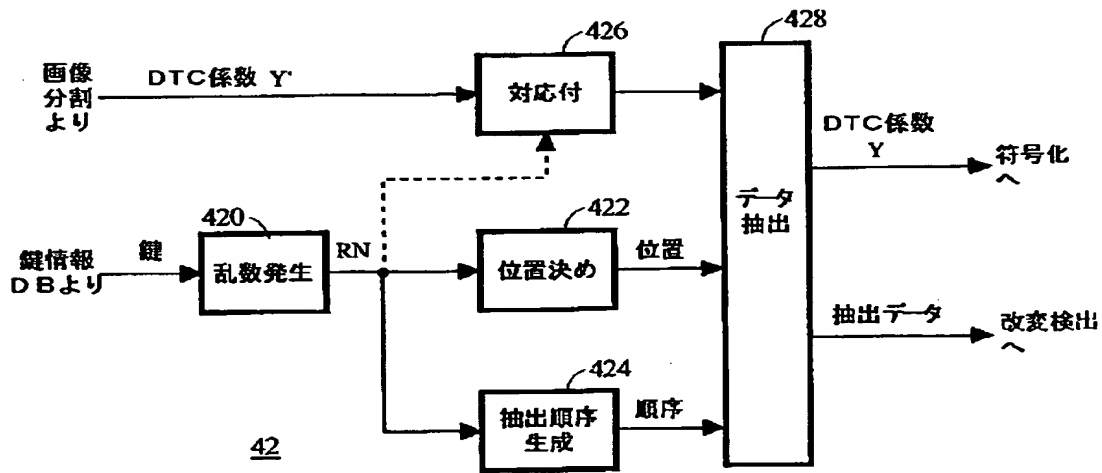
【図 12】



【図 13】

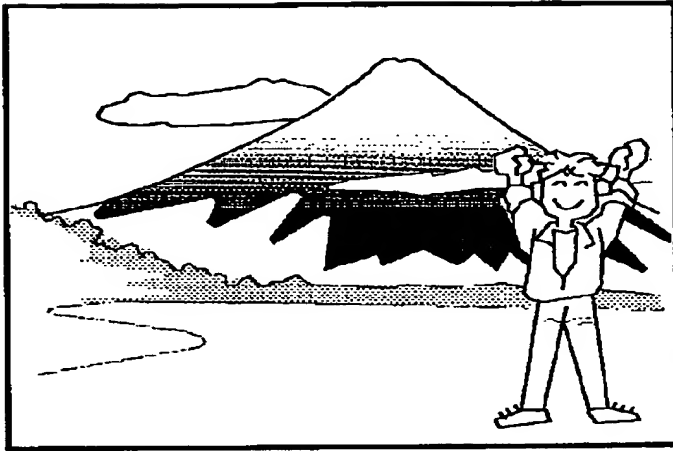


【図 14】

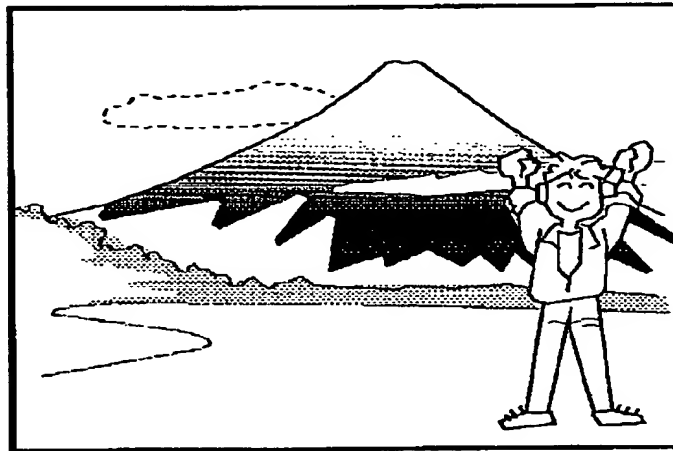


【図 15】

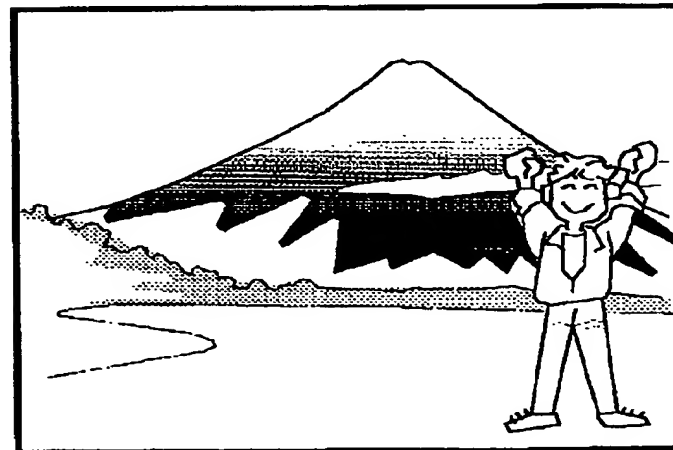
(A)



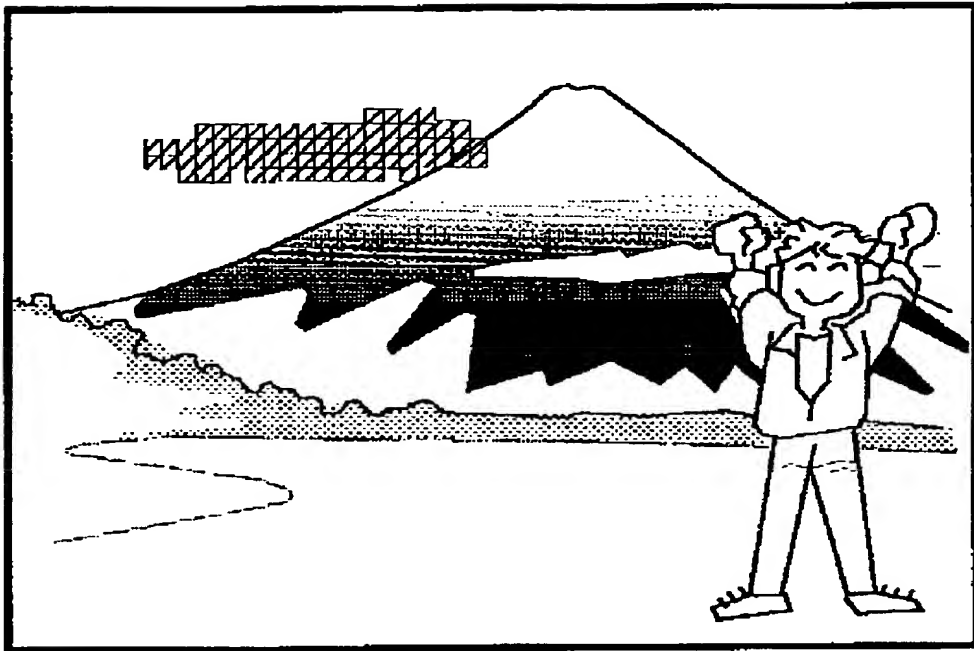
(B)



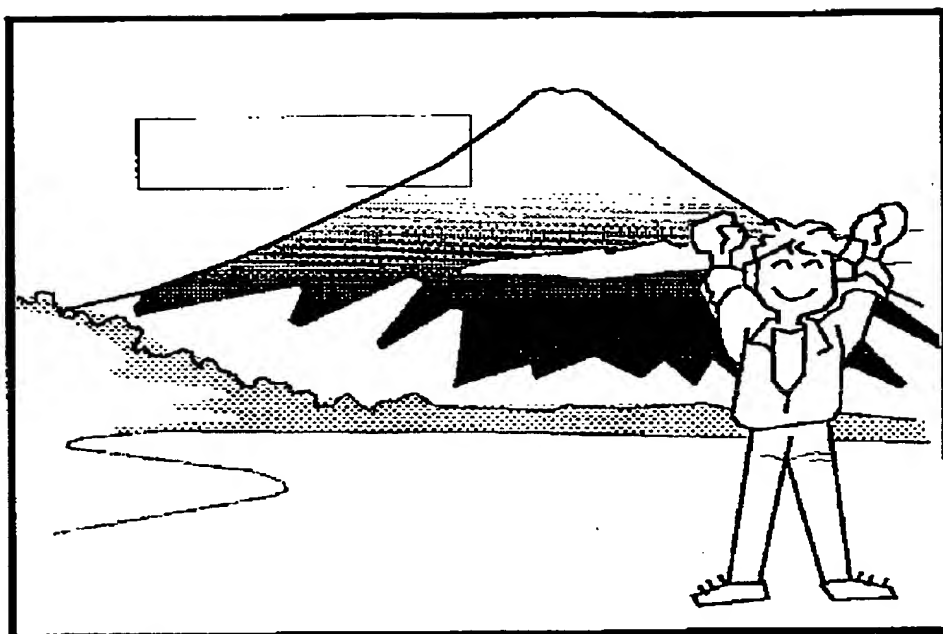
(C)



【図 16】



【図 17】



【図 18】

	1	2	3	4	5		%
ペア 1～96	ペア11 1	ペア5 0	ペア31 1	ペア9 1	0	-----	1
ペア 97～192	ペア99 1	ペア126 0	ペア150 1	ペア153 1	0	-----	1
ペア 193～288	1	0	1	1	0	-----	1
ペア 289～384	1	0	1	1	0	-----	1
⋮	⋮	⋮	⋮	⋮	⋮		⋮
ペア 6049～6144	1	0	1	0	0	-----	1
抽出結果	1	0	1	1	0	-----	1

64 回繰り返し

【図 19】

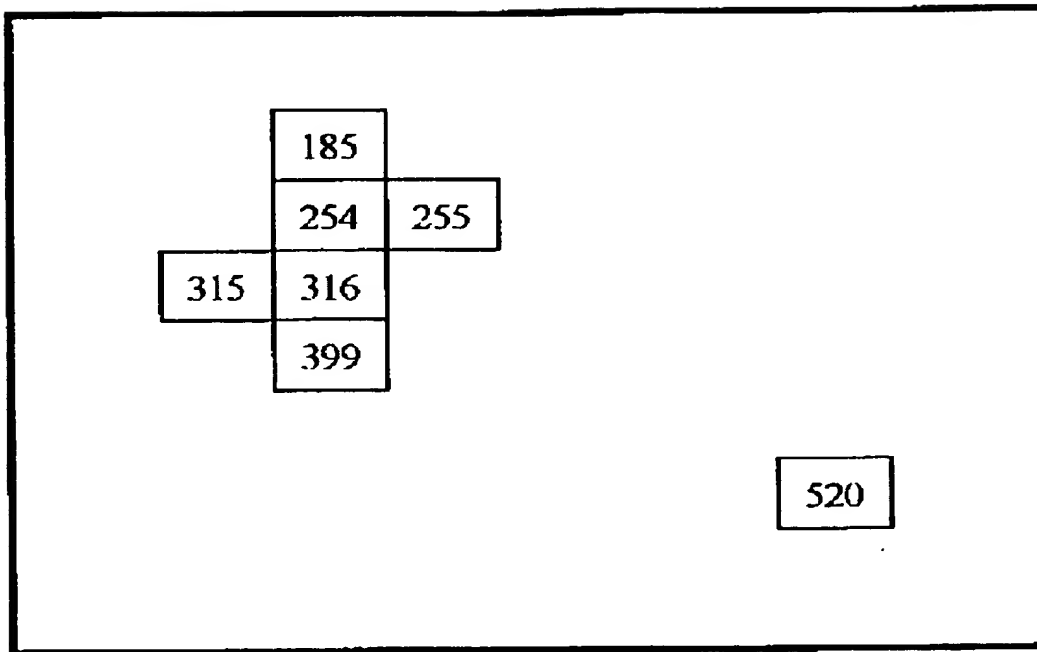
検出埋込データビット番号 (全 96 ビットの埋込データの場合)

	1	2	3	4	5		96
ペア 1~96	ペア11 1	ペア5 0	ペア31 1	ペア9 1	0	-----	1
ペア 97~192	ペア99 1	ペア126 0	ペア150 1	ペア153 1	0	-----	ペア185 0
ペア 193~288	1	0	1	ペア255 0	0	-----	ペア254 0
ペア 289~384	1	ペア315 1	1	1	ペア316 1	-----	1
ペア 385~480	ペア399 0	0	1	1	0	-----	1
ペア 481~576	1	0	1	1	ペア520 1	-----	1
⋮	⋮	⋮	⋮	⋮	⋮		⋮
抽出結果	1	0	1	1	0	-----	1

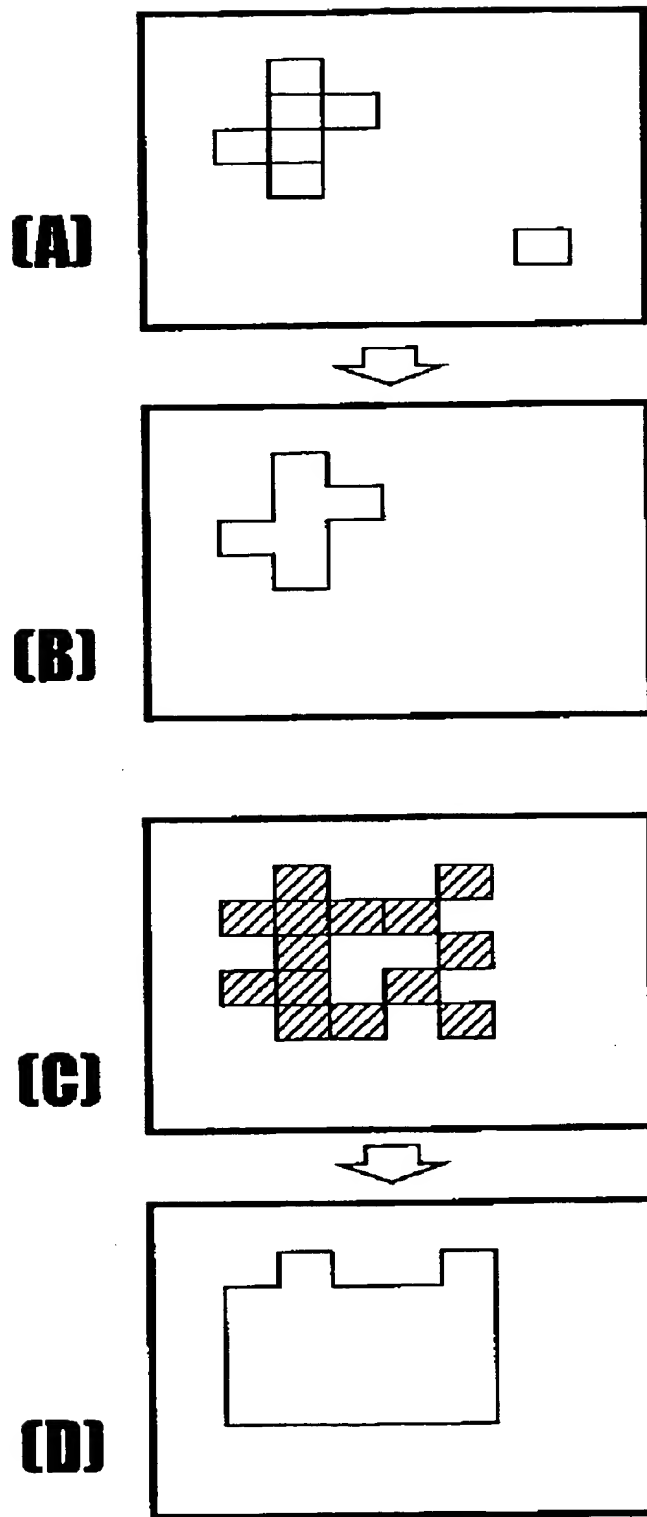


不整合が発見された場合

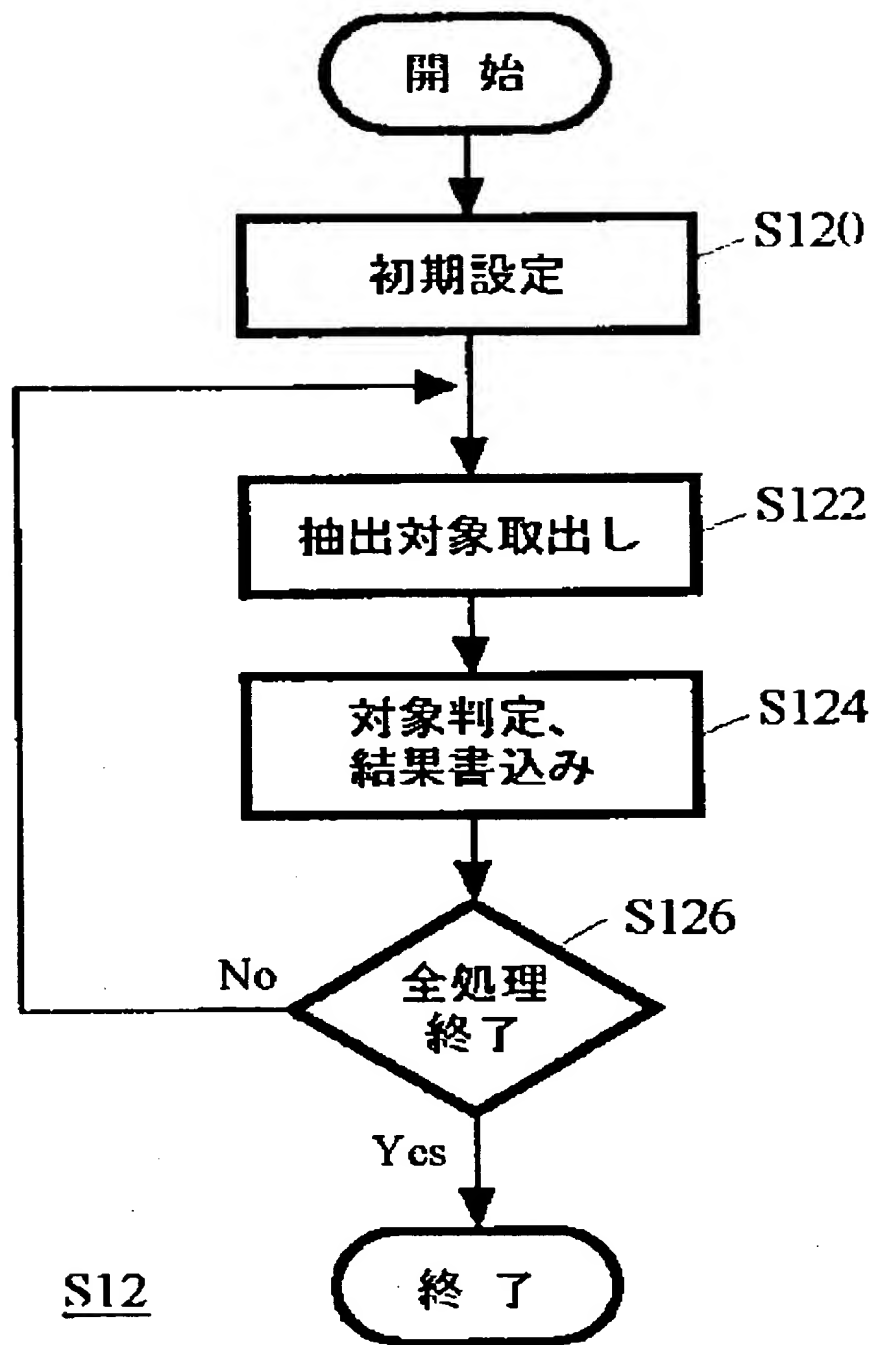
【図 20】



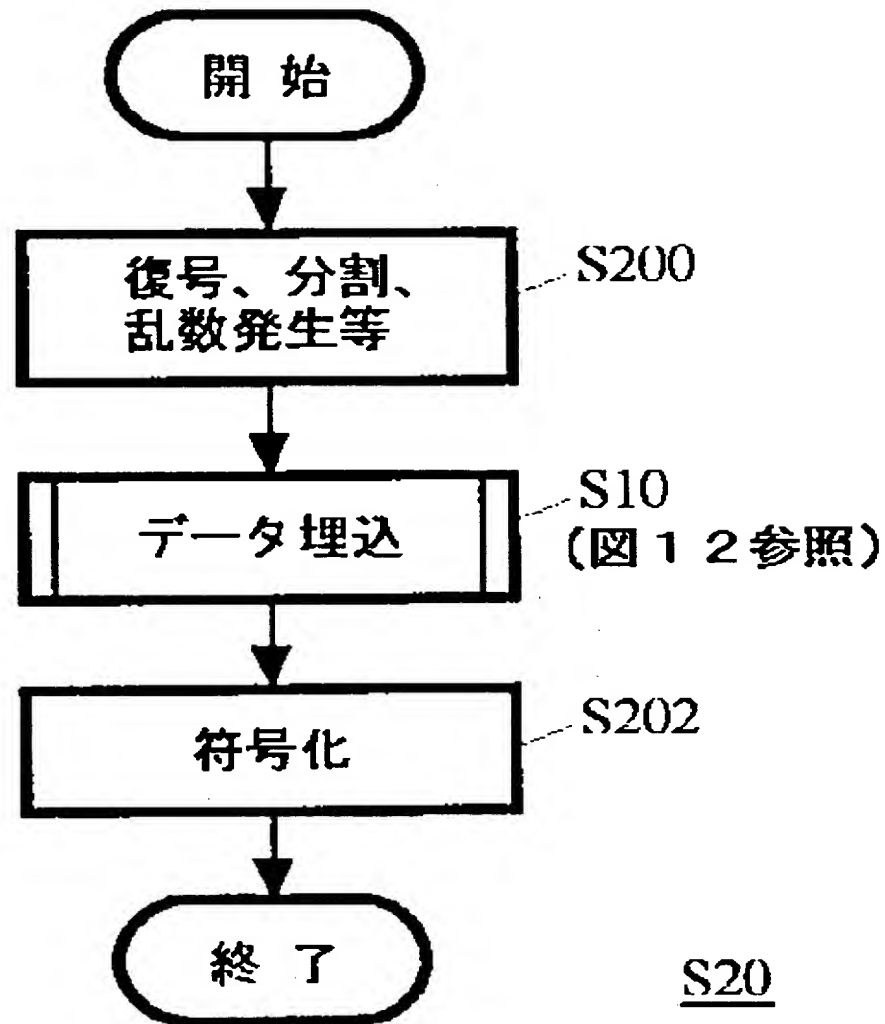
【図 21】



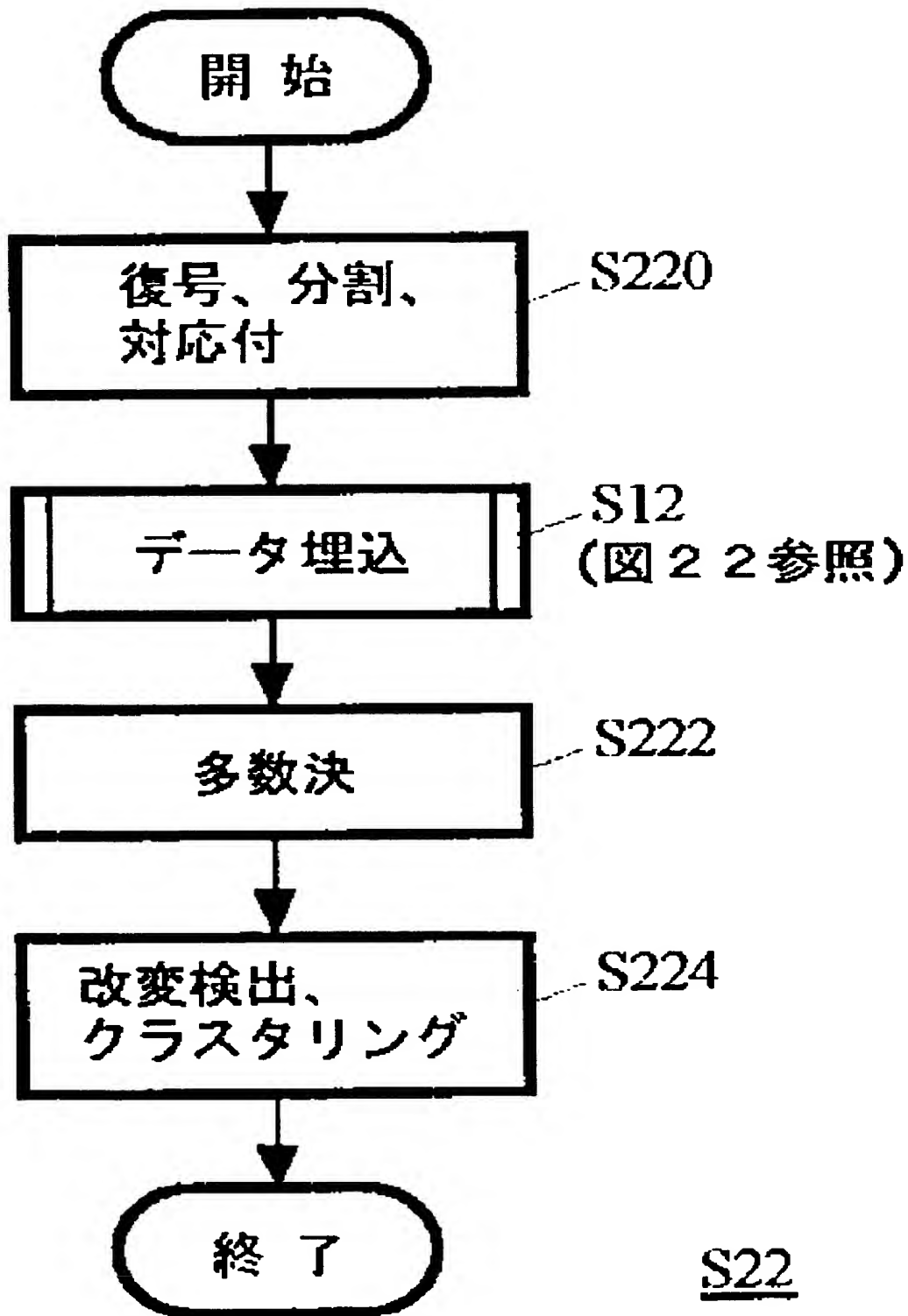
【図 22】



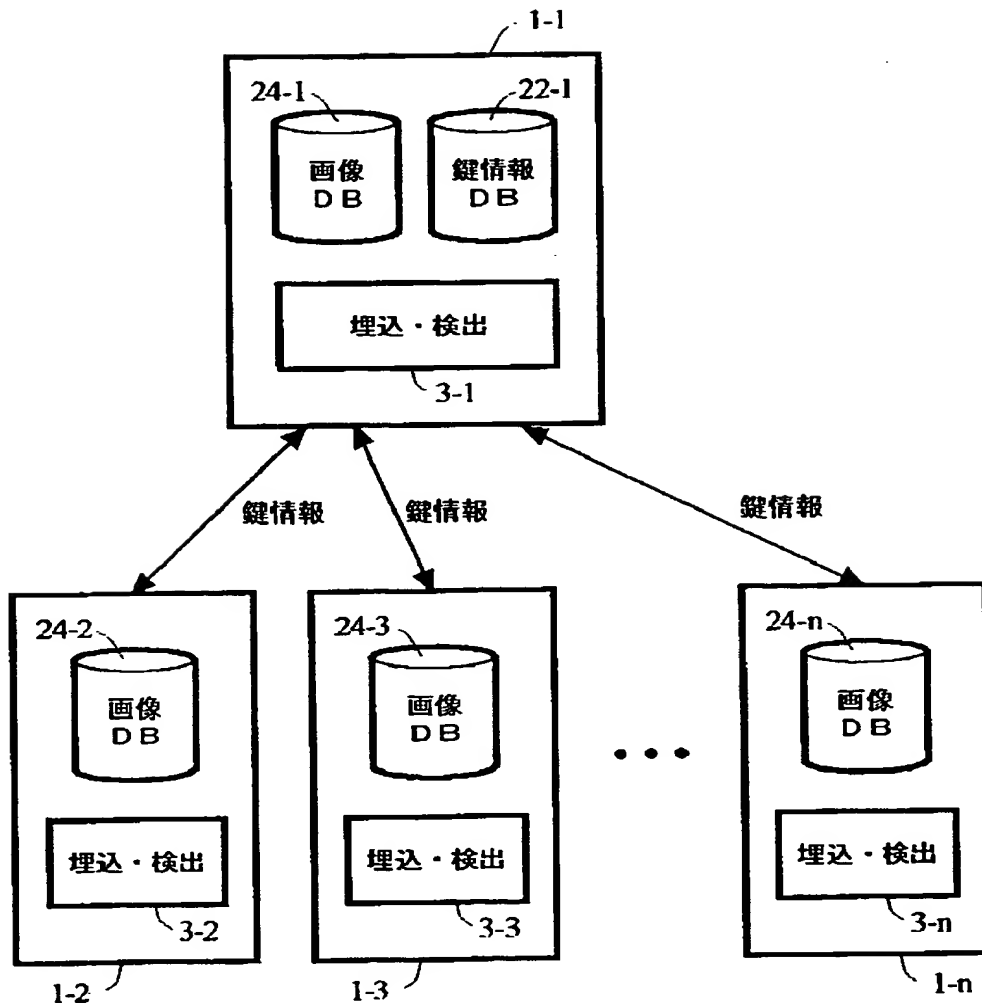
【図 23】



【図 24】



【図 2 5】



【書類名】 要約書

【要約】

【課題】画像に電子透かしを埋め込むことにより、画像のいずれの部分に改変が加えられているかを判定する。

【解決手段】埋込部30は、画像の輝度成分YのDCTブロックを2つずつペアにし、乱数を用いて、各ペアに含まれるDCTブロックそれぞれから、互いに対応するDCT係数をランダムに選択し、これらのDCT係数同士の関係が、所定の規則に従ってデータを表すように操作し、データを埋め込む。この画像に改変が加えられると、改変部分のペアに含まれるDCT係数が、上記規則に従わなくなり、元のデータと異なる値を表すようになる。抽出部40は、画像からデータを抽出し、多数決を採って最初に埋め込まれたデータを推定し、推定したデータと異なるデータが抽出されたペアに改変が加えられたと判定し、表示する。

【選択図】 図2

認定・付加情報

特許出願の番号	平成11年 特許願 第107055号
受付番号	59900354189
書類名	特許願
担当官	第三担当上席 0092
作成日	平成11年 4月16日

<認定情報・付加情報>

【提出日】	平成11年 4月14日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 1990年10月24日

[変更理由] 新規登録

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレイション